



This is a digital copy of a book that was preserved for generations on library shelves before it was carefully scanned by Google as part of a project to make the world's books discoverable online.

It has survived long enough for the copyright to expire and the book to enter the public domain. A public domain book is one that was never subject to copyright or whose legal copyright term has expired. Whether a book is in the public domain may vary country to country. Public domain books are our gateways to the past, representing a wealth of history, culture and knowledge that's often difficult to discover.

Marks, notations and other marginalia present in the original volume will appear in this file - a reminder of this book's long journey from the publisher to a library and finally to you.

Usage guidelines

Google is proud to partner with libraries to digitize public domain materials and make them widely accessible. Public domain books belong to the public and we are merely their custodians. Nevertheless, this work is expensive, so in order to keep providing this resource, we have taken steps to prevent abuse by commercial parties, including placing technical restrictions on automated querying.

We also ask that you:

- + *Make non-commercial use of the files* We designed Google Book Search for use by individuals, and we request that you use these files for personal, non-commercial purposes.
- + *Refrain from automated querying* Do not send automated queries of any sort to Google's system: If you are conducting research on machine translation, optical character recognition or other areas where access to a large amount of text is helpful, please contact us. We encourage the use of public domain materials for these purposes and may be able to help.
- + *Maintain attribution* The Google "watermark" you see on each file is essential for informing people about this project and helping them find additional materials through Google Book Search. Please do not remove it.
- + *Keep it legal* Whatever your use, remember that you are responsible for ensuring that what you are doing is legal. Do not assume that just because we believe a book is in the public domain for users in the United States, that the work is also in the public domain for users in other countries. Whether a book is still in copyright varies from country to country, and we can't offer guidance on whether any specific use of any specific book is allowed. Please do not assume that a book's appearance in Google Book Search means it can be used in any manner anywhere in the world. Copyright infringement liability can be quite severe.

About Google Book Search

Google's mission is to organize the world's information and to make it universally accessible and useful. Google Book Search helps readers discover the world's books while helping authors and publishers reach new audiences. You can search through the full text of this book on the web at <http://books.google.com/>



Über dieses Buch

Dies ist ein digitales Exemplar eines Buches, das seit Generationen in den Regalen der Bibliotheken aufbewahrt wurde, bevor es von Google im Rahmen eines Projekts, mit dem die Bücher dieser Welt online verfügbar gemacht werden sollen, sorgfältig gescannt wurde.

Das Buch hat das Urheberrecht überdauert und kann nun öffentlich zugänglich gemacht werden. Ein öffentlich zugängliches Buch ist ein Buch, das niemals Urheberrechten unterlag oder bei dem die Schutzfrist des Urheberrechts abgelaufen ist. Ob ein Buch öffentlich zugänglich ist, kann von Land zu Land unterschiedlich sein. Öffentlich zugängliche Bücher sind unser Tor zur Vergangenheit und stellen ein geschichtliches, kulturelles und wissenschaftliches Vermögen dar, das häufig nur schwierig zu entdecken ist.

Gebrauchsspuren, Anmerkungen und andere Randbemerkungen, die im Originalband enthalten sind, finden sich auch in dieser Datei – eine Erinnerung an die lange Reise, die das Buch vom Verleger zu einer Bibliothek und weiter zu Ihnen hinter sich gebracht hat.

Nutzungsrichtlinien

Google ist stolz, mit Bibliotheken in partnerschaftlicher Zusammenarbeit öffentlich zugängliches Material zu digitalisieren und einer breiten Masse zugänglich zu machen. Öffentlich zugängliche Bücher gehören der Öffentlichkeit, und wir sind nur ihre Hüter. Nichtsdestotrotz ist diese Arbeit kostspielig. Um diese Ressource weiterhin zur Verfügung stellen zu können, haben wir Schritte unternommen, um den Missbrauch durch kommerzielle Parteien zu verhindern. Dazu gehören technische Einschränkungen für automatisierte Abfragen.

Wir bitten Sie um Einhaltung folgender Richtlinien:

- + *Nutzung der Dateien zu nichtkommerziellen Zwecken* Wir haben Google Buchsuche für Endanwender konzipiert und möchten, dass Sie diese Dateien nur für persönliche, nichtkommerzielle Zwecke verwenden.
- + *Keine automatisierten Abfragen* Senden Sie keine automatisierten Abfragen irgendwelcher Art an das Google-System. Wenn Sie Recherchen über maschinelle Übersetzung, optische Zeichenerkennung oder andere Bereiche durchführen, in denen der Zugang zu Text in großen Mengen nützlich ist, wenden Sie sich bitte an uns. Wir fördern die Nutzung des öffentlich zugänglichen Materials für diese Zwecke und können Ihnen unter Umständen helfen.
- + *Beibehaltung von Google-Markenelementen* Das "Wasserzeichen" von Google, das Sie in jeder Datei finden, ist wichtig zur Information über dieses Projekt und hilft den Anwendern weiteres Material über Google Buchsuche zu finden. Bitte entfernen Sie das Wasserzeichen nicht.
- + *Bewegen Sie sich innerhalb der Legalität* Unabhängig von Ihrem Verwendungszweck müssen Sie sich Ihrer Verantwortung bewusst sein, sicherzustellen, dass Ihre Nutzung legal ist. Gehen Sie nicht davon aus, dass ein Buch, das nach unserem Dafürhalten für Nutzer in den USA öffentlich zugänglich ist, auch für Nutzer in anderen Ländern öffentlich zugänglich ist. Ob ein Buch noch dem Urheberrecht unterliegt, ist von Land zu Land verschieden. Wir können keine Beratung leisten, ob eine bestimmte Nutzung eines bestimmten Buches gesetzlich zulässig ist. Gehen Sie nicht davon aus, dass das Erscheinen eines Buchs in Google Buchsuche bedeutet, dass es in jeder Form und überall auf der Welt verwendet werden kann. Eine Urheberrechtsverletzung kann schwerwiegende Folgen haben.

Über Google Buchsuche

Das Ziel von Google besteht darin, die weltweiten Informationen zu organisieren und allgemein nutzbar und zugänglich zu machen. Google Buchsuche hilft Lesern dabei, die Bücher dieser Welt zu entdecken, und unterstützt Autoren und Verleger dabei, neue Zielgruppen zu erreichen. Den gesamten Buchtext können Sie im Internet unter <http://books.google.com> durchsuchen.

math 1509.02.7
A



Harvard College Library

BOUGHT WITH THE INCOME

FROM THE BEQUEST OF

PROF. JOHN FARRAR, LL.D.

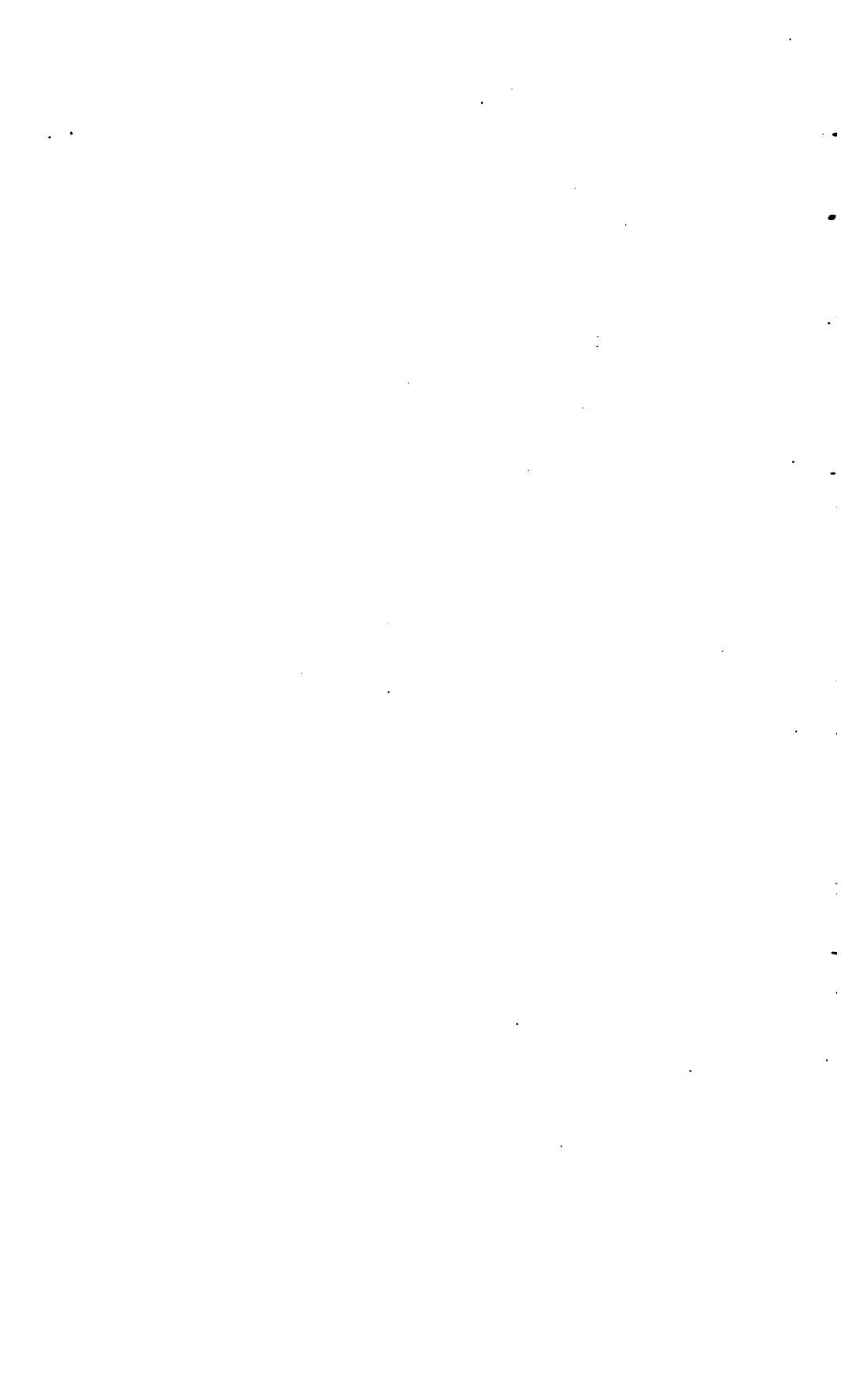
AND HIS WIDOW

ELIZA FARRAR

FOR

"BOOKS IN THE DEPARTMENT OF MATHEMATICS,
ASTRONOMY, AND NATURAL PHILOSOPHY"







1939

ANFANGSGRÜNDE
DER
ZAHLENLEHRE





Pierre de Fermat

(1601 — 1665).

Nach einem Stich von F. Poilly.

©

ANFANGSGRÜNDE

DER

ZAHLENLEHRE

VON

GUSTAV WERTHEIM

MIT DEN BILDNISSEN VON FERMAT, LAGRANGE,
EULER UND GAUß

BRAUNSCHWEIG

DRUCK UND VERLAG VON FRIEDRICH VIEWEG UND SOHN

1902

math 1509.02.7
A

1887

Farrar fund.

Alle Rechte, namentlich dasjenige der Übersetzung in fremde Sprachen,
vorbehalten

V O R W O R T.

Bei der Abfassung meiner „Elemente der Zahlentheorie“, die 1887 im Verlage von B. G. Teubner in Leipzig erschienen sind, hatte ich mir die Aufgabe gestellt, Studierende der Mathematik auf möglichst einfache Weise in den Gegenstand einzuführen und mit ihnen so weit wie die Anfangsvorlesungen zu gehen, die auf den Universitäten über den Gegenstand gehalten werden. Meine „Elemente“ behandeln deshalb noch die binären quadratischen Formen und die auf der Theorie dieser Formen beruhende ganzzahlige Auflösung der allgemeinen Gleichung zweiten Grades mit zwei Unbekannten. Das vorliegende Buch geht nicht so weit, auch setzt es einen anderen Leserkreis voraus. Es wendet sich nicht gerade an Studierende der Mathematik, sondern soll Gebildete aller Stände, die Interesse für die Zahlenlehre haben, mit den wichtigsten Sätzen und Methoden derselben vertraut machen, soweit sie sich mittels der Elementar-Mathematik, wie sie unsere Gymnasien und Realschulen übermitteln, begründen lassen. Die Rücksicht auf diesen Zweck mußte die Auswahl des Stoffes und die Art der Darstellung beeinflussen. Ob ich nach diesen beiden Richtungen hin das Richtige getroffen habe, muß ich dem Urteil der Sachverständigen überlassen.

Was die Auswahl des Stoffes betrifft, so bemerke ich noch Folgendes: Wer einem bestimmten Ziele zustrebt, das er möglichst schnell erreichen will, um sodann zu einem weiter entfernten Punkte hinzueilen, wird manches übergehen oder nur kurz berühren können, bei dem ein anderer, dem überhaupt kaum daran gelegen ist, wie weit er komme, sondern der — unbekümmert um ein Endziel — sich aus Freude an der Sache mit einer Wissen-

schaft beschäftigen will, länger und behaglicher verweilen kann. So erklärt es sich, daß ich jetzt einige Punkte eingehend behandelt habe, denen ich in meinem früheren Werke nur wenige Zeilen widmen konnte. Dahin gehört u. a. die Theorie der „vollkommenen Zahlen“. Der Gegenstand ist freilich veraltet; aber er hat mehr als 2000 Jahre die größten Denker beschäftigt; noch Fermat, der Begründer der modernen Zahlenlehre, hat ihn sorgfältiger Untersuchungen nicht für unwert gehalten, und deshalb schien es mir nicht überflüssig, das Wichtigste, was darüber ermittelt worden ist, zusammenzustellen.

Dem immer mehr steigenden Interesse für die Geschichte der Mathematik habe ich auf verschiedene Arten Rechnung zu tragen gesucht: Ich habe einige der mathematischen Klassiker — so Euklid, Euler, Lagrange, Legendre, Gauß — hin und wieder selbst reden lassen, ohne daß dadurch — wie ich hoffe — die Einheitlichkeit der Darstellung gelitten hat. Ferner habe ich vielfach auch die Quellen angegeben, aus denen ich geschöpft habe und zwar — soweit es mir hier¹⁾ möglich war — die Originalschriften selbst, nicht Darstellungen, deren Verfasser häufig nur mehr oder weniger unzuverlässige Berichte benutzen konnten. Es ist nämlich gar nicht selten, daß eine Angabe ungeprüft von einem Buch in ein anderes übergeht, weil die Quelle, aus welcher der erste Verbreiter sie entnommen hat, nicht angegeben, eine Prüfung also erschwert, wenn nicht unmöglich gemacht ist. Auf diese Weise werden leicht Irrtümer so weit verbreitet, daß jeder sie für Wahrheiten hält und es schwer ist, sie auszurotten. Ich habe mich bemüht, durch korrekte Citate diesem Übelstande vorzubeugen. Endlich sind noch zur Förderung des historischen Sinnes die Aufgaben, die ich zur Einübung der Sätze und Methoden gebe, wo es nur immer anging, aus mathematischen Klassikern entnommen, u. a. auch aus der Arithmetik des noch immer nicht genügend bekannten Diophant, dessen Studium, obwohl seine Lösungen nicht allgemein sind, jedem, der Muße hat sich mit ihm zu beschäftigen, einen hohen Genuß bereiten wird.

¹⁾ In der reichen Stadt Frankfurt a. M. gibt es zur Zeit keine öffentliche Bibliothek, welche mathematische Bücher kauft.

Die Tabellen des Anhangs konnten zwar aus Rücksicht auf den verfügbaren Raum nur eine geringe Ausdehnung erhalten, sie werden aber bei der Lösung von Übungsaufgaben nicht unwillkommen sein. Es war meine Absicht gewesen, für jede Primzahl unter 10 000 die kleinste primitive Wurzel zu berechnen; mein Gesundheitszustand hat mir jedoch einen Strich durch die Rechnung gemacht. Die Bezeichnung der Primzahlen, für welche 10 eine primitive Wurzel ist, ist nach Kefslers Tabelle erfolgt.

Die Beschränkung der Indizestafeln auf die Zahlen unter 100 hat eine bequemere Anordnung gestattet, als bei einer größeren Ausdehnung möglich gewesen wäre. Übrigens sind in dieselben auch die zusammengesetzten Moduln aufgenommen, welche die Anwendung von Indizes zulassen.

Die schöne graphische Darstellung des Reziprozitätssatzes für die Primzahlen unter 100 habe ich einer Arbeit des vor einigen Jahren verstorbenen französischen Ingenieurs Adolphe Matrot entnommen.

Zum Schluss erübrigt mir noch, der Verlagsbuchhandlung, die ohne Rücksicht auf die Kosten — wie u. a. die dem Buche beigelegten Bildnisse von Fermat, Lagrange, Euler und Gauß zeigen — jedem meiner Wünsche bereitwilligst entsprochen hat, meinen wärmsten Dank auszusprechen.

Frankfurt a. M., 19. August 1902.

Gustav Wertheim.

INHALTSVERZEICHNIS.

Erstes Kapitel.

Teilbarkeit der Zahlen.

	Seite
§. 1. Zahlensysteme	1
§. 2. Das dyadische System	3
§. 3. Formen der Zahlen	6
§. 4. Primzahlen und zusammengesetzte Zahlen	6
§. 5. Sätze über die Formen von Primzahlen	7
§. 6. Anzahl der Primzahlen	8
§. 7. Ermittlung der Primzahlen	11
§. 8. Darstellung der Primzahlen durch Polynome	13
§. 9. Primzahlen gleicher Differenz	14
§. 10. Darstellung der Zahlen als Summen aufeinander folgender Zahlen	16
§. 11. Darstellung der Zahlen als Differenz zweier Quadrate	17
§. 12. Zusammengesetzte Zahlen und Zerlegung derselben in Faktoren	19
§. 13. Divisoren einer Zahl. Anzahl, Summe und Produkt derselben .	23
§. 14. Vollkommene Zahlen	27
§. 15. Befreundete Zahlen	32
§. 16. Der grösste gemeinschaftliche Divisor von Zahlen. — Relative Primzahlen	32
§. 17. Sätze über relative Primzahlen	35
§. 18. Das kleinste Vielfache von Zahlen	38
§. 19. Über die Anzahl der Zahlen, welche prim zu einer Zahl und nicht gröfser als dieselbe sind. Summe dieser Zahlen	42
§. 20. Höchste Potenz einer Primzahl, welche in dem Produkt aller Zahlen von 1 bis n aufgeht	50
§. 21. Anzahl der Zahlen eines gegebenen Gebiets, welche durch ge- gebene Primzahlen nicht teilbar sind	54
§. 22. Über die Anzahl der Primzahlen zwischen 1 und einer beliebigen Zahl n	58
Anhang. Meissels Zählung der Primzahlen eines gegebenen Gebiets	59

Zweites Kapitel.

Kongruente Zahlen.

§. 23. Definition kongruenter Zahlen	64
§. 24. Reste einer Zahl	65

Inhaltsverzeichnis.

IX

	Seite
§. 25. Das vollständige Restsystem in Beziehung auf einen Modul . .	66
§. 26. Kongruenzen	67
§. 27. Sätze über die Verbindung von Kongruenzen	67
§. 28. Rechnungsproben	71
§. 29. Teilbarkeitsregeln	72
§. 30. Aufgaben	77
§. 31. Berechnung des Osterfestes	79
§. 32. Umformung einer Kongruenz	81
§. 33. Wurzeln von Kongruenzen	82

Drittes Kapitel.

Kongruenzen ersten Grades.

§. 34. Die Kongruenz ersten Grades mit einer Unbekannten. — Anzahl ihrer Wurzeln	85
§. 35. Auflösung der Kongruenz ersten Grades mit einer Unbekannten	88
§. 36. Zurückführung der Kongruenzen ersten Grades, deren Moduln zusammengesetzte Zahlen sind, auf solche mit Primzahlmoduln	94
§. 37. Anwendungen der Kongruenzen ersten Grades	96
§. 38. Zahlen, welche für gegebene Moduln gegebene Reste liefern . .	98
§. 39. Zerlegung eines Bruches in seine Partialbrüche	103
§. 40. Auflösung der Gleichung $Ax + By + Cz + \dots = \mu$, in welcher μ der größte gemeinschaftliche Divisor der Zahlen $A, B, C, \dots$ ist	105
§. 41. Auflösung der Kongruenz ersten Grades mit mehreren Unbekannten	108
§. 42. Auflösung eines Systems von m Kongruenzen ersten Grades mit m oder mehr Unbekannten	111
§. 43. Der Wilsonsche Satz (Beweise von Lagrange, Gauß, Stern)	114
§. 44. Der Fermatsche Satz [Beweise von Euler, Lambert, Lagrange, Laplace, Gauß (Leibnitz), Lejeune Dirichlet]	119
§. 45. Anwendungen des Fermat'schen Satzes (Lagranges zweiter Beweis des Wilsonschen Satzes. Auflösung der Kongruenz ersten Grades mit einer Unbekannten)	124
§. 46. Summe der Reste der Vielfachen einer Zahl	126
§. 47. Anzahl der Wurzeln einer Kongruenz, deren Modul eine Primzahl ist. (Fünfter Beweis des Wilsonschen Satzes)	127

Viertes Kapitel.

Einige unbestimmte Gleichungen höherer Grade. — Die Gleichung $x^y = y^x$. — Aufgaben.

§. 48. Auflösung der unbestimmten Gleichung zweiten Grades mit zwei Unbekannten, von denen die eine nur im ersten Grade vorkommt	134
§. 49. Die Pythagoreische Gleichung. Heronische Zahlen	137

	Seite
§. 50. Die Gleichung $a + bx + cx^2 = y^2$. Aufgaben	141
§. 51. Die Gleichung $ax^2 + by^2 = z^2$	149
§. 52. Die Gleichung $x^y = y^x$	150
§. 53. Aufgaben	151

Fünftes Kapitel.

Die Kettenbrüche und ihre Anwendung auf die Zahlenlehre.

§. 54. Historisches. — Entstehung der Kettenbrüche	164
§. 55. Verwandlung eines rationalen Bruchs in einen Kettenbruch . .	169
§. 56. Bildung der Näherungsbrüche	173
§. 57. Eigenschaften der Näherungsbrüche	178
§. 58. Eingeschaltete Näherungsbrüche	182
§. 59. Umkehrung der Kettenbrüche	185
§. 60. Symmetrische Kettenbrüche	187
§. 61. Zerfällung von Zahlen in zwei Quadrate	189
§. 62. Auflösung der Kongruenz ersten Grades mit einer Unbekannten	196
§. 63. Irrationale Gröſsen, deren Entwicklungen in Kettenbrüche zu einem und demselben vollständigen Quotienten führen	198
§. 64. Periodische Kettenbrüche	200
§. 65. Verwandlung der irrationalen Wurzeln gemischt quadratischer Gleichungen in Kettenbrüche	202
§. 66. Sätze über die Kettenbrüche, welche die irrationalen Wurzeln gemischt quadratischer Gleichungen darstellen	208
§. 67. Verwandlung der irrationalen Wurzeln einer rein quadratischen Gleichung in Kettenbrüche	213
§. 68. Die Fermatsche Aufgabe	219

Sechstes Kapitel.

Potenzreste für Primzahlmoduln.

§. 69. Berechnung der Potenzreste	227
§. 70. Der Exponent, zu welchem eine Zahl a für den Modul p gehört	228
§. 71. Die Periode einer Zahl für einen Modul	230
§. 72. Eulers zweiter Beweis des Fermatschen Satzes	232
§. 73. Verteilung der durch p nicht teilbaren Zahlen unter die verschiedenen Divisoren von $p - 1$ als Exponenten	233
§. 74. Produkt der zu demselben Exponenten gehörenden Zahlen . .	238
§. 75. Primitive Wurzeln	238
§. 76. Berechnung einer primitiven Wurzel der Primzahl p	240
§. 77. Indizes	243
§. 78. Auflösung der Kongruenz ersten Grades mittels der Indizes . .	245
§. 79. Die binomische Kongruenz. — Auflösung derselben mittels der Indizes	247
§. 80. Die Exponential-Kongruenz	250
§. 81. Zusammenhang zwischen den für zwei verschiedene primitive Wurzeln genommenen Indizes einer Zahl	251

	Seite
§. 82. Die Indizes einer Zahl und der Exponent, zu welchem die Zahl gehört	253
§. 83. Summe und Produkt der Glieder der Periode einer Zahl. — Eulers Beweis des Wilsonschen Satzes	256
§. 84. Produkt der primitiven Wurzeln einer Primzahl. — Summe der Indizes einer Zahl	258
§. 85. Summe der zu einem Exponenten gehörenden Zahlen. — Summe der primitiven Wurzeln einer Primzahl	259
§. 86. Aufgaben	263

Siebentes Kapitel.

Potenzreste für zusammengesetzte Moduln.

§. 87. Der Exponent, zu welchem eine Zahl für einen Modul gehört	268
§. 88. Der verallgemeinerte Fermatsche Satz. Auflösung der Kongruenz ersten Grades mit einer Unbekannten	269
§. 89. Verteilung der Zahlen, die prim zu m sind, unter die Divisoren von $\varphi(m)$ als Exponenten	271
§. 90. Zahlen, welche keine primitiven Wurzeln besitzen können . .	275
§. 91. Primitive Wurzeln einer Potenz einer ungeraden Primzahl . .	277
§. 92. Primitive Wurzeln von $2p^2$	283
§. 93. Verteilung der Zahlen, die prim zu p^2 , resp. $2p^2$ sind, unter die Divisoren von $\varphi(p^2) = \varphi(2p^2) = (p-1)p^{2-1}$ als Exponenten	284
§. 94. Indizes. Auflösung der Kongruenz ersten Grades und der binomischen Kongruenz für die Moduln p^2 und $2p^2$	287
§. 95. Der Modul 2^x . — Verteilung der Zahlen, die prim zu 2^x und kleiner als 2^x sind, unter die Divisoren von 2^{x-2}	289
§. 96. Indizes, wenn der Modul eine Potenz von 2 ist	292
§. 97. Anwendung der Indizes zur Auflösung der linearen und der binomischen Kongruenz für den Modul 2^x , ...	294
§. 98. Die binomische Kongruenz im Falle eines beliebig zusammengesetzten Moduls	295
§. 99. Über die Divisoren der Zahl $a^m - 1$	297
§. 100. Über die Divisoren der Zahl $a^m + 1$	300
§. 101. Verwandlung gemeiner Brüche in Dezimalbrüche	303
§. 102. Aufgaben	311

Achtes Kapitel.

Kongruenzen zweiten Grades.

§. 103. Auflösung der rein quadratischen Kongruenz	317
§. 104. Verwandlung der gemischt quadratischen Kongruenz mit einer Unbekannten in eine rein quadratische	318
§. 105. Quadratische Reste und Nichtreste	322
§. 106. Reste einer ungeraden Primzahl	325
§. 107. Reste einer Potenz einer ungeraden Primzahl	327
§. 108. Das Produkt aller Zahlen, die prim zu p^2 und $< p^2$ sind . .	331

	Seite
§. 109. Eulers Kriterium zu entscheiden, ob eine Zahl Rest oder Nichtrest einer ungeraden Primzahl oder einer Potenz einer solchen sei	332
§. 110. Quadratischer Charakter eines Produkts	335
§. 111. Reste der Potenzen von 2	338
§. 112. Die rein quadratische Kongruenz für einen beliebig zusammengesetzten Modul	341
§. 113. Der verallgemeinerte Wilson'sche Satz	343
§. 114. Für welche Moduln ist eine gegebene Zahl Rest, und für welche ist sie Nichtrest?	345
§. 115. Moduln, für welche -1 quadratischer Rest ist	347
§. 116. Moduln, für welche $+2$ quadratischer Rest ist	350
§. 117. Gauß's Kriterium zu entscheiden, ob eine gegebene Zahl Rest oder Nichtrest einer ungeraden Primzahl sei	355
§. 118. Anwendungen des Gauß'schen Kriteriums	357
§. 119. Der Reziprozitätssatz	360
§. 120. Beweis des Reziprozitätssatzes	362
§. 121. Divisoren von $x^2 - a$ für den Fall, daß a eine Primzahl ist	367
§. 122. Divisoren von $x^2 - A$ für den Fall, daß A eine zusammengesetzte Zahl ist	378
§. 123. Auflösung der rein quadratischen Kongruenz	378
§. 124. Die Kongruenz $x^2 \equiv a \pmod{m}$, wenn a nicht prim zu m ist	383
§. 125. Über die Aufeinanderfolge der Reste und Nichtreste der Primzahl p in der Reihe $1, 2, 3, \dots, p-1$	385
§. 126. Auflösung der Kongruenz $ax^2 + by^2 \equiv c \pmod{p}$	388
§. 127. Matrots Bestimmung der Primzahlen, für welche $+2$ Rest ist	391
§. 128. Der Bachetsche Satz	398
§. 129. Aufgaben	398
Zusätze	400
Anhang	405
Namen- und Sachregister	423

Erstes Kapitel.

Teilbarkeit der Zahlen.

§. 1.

Zahlensysteme.

Man bildet ein Zahlensystem für die Grundzahl (Basis) g , indem man alle Zahlen m auf die Form

$$m = \dots a_3 g^3 + a_2 g^2 + a_1 g + a_0$$

bringt, wo $\dots g^3, g^2, g$ die Potenzen von g und $\dots a_3, a_2, a_1, a_0$ ganze positive Zahlen $< g$ bezeichnen, deren Zeichen man die Ziffern im System der Basis g nennt. Mit Ausnahme der Einheit kann man jede ganze positive Zahl zur Basis wählen; so z. B. wird die Zahl siebenundzwanzig für die Basis

2 dargestellt durch $1.2^4 + 1.2^3 + 0.2^2 + 1.2 + 1$, also geschrieb. 11011;						
3	"	"	1.3^3 ,	"	"	1000;
4	"	"	$1.4^3 + 2.4 + 3$,	"	"	123;
5	"	"	$1.5^3 + 0.5 + 2$,	"	"	102;
6	"	"	$4.6 + 3$,	"	"	43;
7	"	"	$3.7 + 6$,	"	"	36;
8	"	"	$3.8 + 3$,	"	"	33;
9	"	"	3.9 ,	"	"	30;
10	"	"	$2.10 + 7$,	"	"	27;
elf = α	"	"	$2.\alpha + 5$,	"	"	25;
zwölf = β	"	"	$2.\beta + 3$,	"	"	23;

Thatsächlich bedient man sich überall des Systems mit der Basis 10 (des dekadischen Systems); es ist aber interessant und

lehrreich, dekadisch geschriebene Zahlen in anderen Systemen auszudrücken und umgekehrt.

1. Aufgabe. Eine dekadisch geschriebene Zahl m im System der Basis g auszudrücken.

Lösung. Man dividiere m durch g ; das gebe den Quotienten q_1 und den Rest r_0 , so daß also $m = q_1 g + r_0$ ist. Weiter dividiere man q_1 durch g , wobei sich der Quotient q_2 und der Rest r_1 ergebe; dann ist

$$q_1 = q_2 g + r_1, \text{ also } m = q_2 g^2 + r_1 g + r_0.$$

In dieser Weise fahre man fort, bis ein Quotient q_n erscheint, der kleiner als g ist; der zugehörige Rest sei r_{n-1} . Dann ist

$$m = q_n g^n + r_{n-1} g^{n-1} + r_{n-2} g^{n-2} + \dots + r_1 g + r_0,$$

geschrieben

$$q_n r_{n-1} r_{n-2} \dots r_1 r_0,$$

der Ausdruck der Zahl m im System der Basis g .

Beispiel. Die dekadisch geschriebene Zahl 30382 im System der Basis 8 auszudrücken. Es ist

$$\begin{array}{rcl} 30382 : 8 & = & 3797, \text{ Rest } 6, \\ 3797 : 8 & = & 474, \quad \text{ „ } 5, \\ 474 : 8 & = & 59, \quad \text{ „ } 2, \\ 59 : 8 & = & 7, \quad \text{ „ } 3, \end{array}$$

also ist

$$30382 \text{ (dekadisch)} = 73256 \text{ (oktadisch)}.$$

2. Aufgabe. Die im System der Basis g geschriebene Zahl

$$m = a_4 g^4 + a_3 g^3 + a_2 g^2 + a_1 g + a_0$$

dekadisch zu schreiben.

Lösung. Statt die Werte der verschiedenen Potenzen von g zu berechnen, dann die vorgeschriebenen Multiplikationen auszuführen und endlich die erhaltenen Produkte zu addieren, rechnet man vorteilhaft nach der Formel

$$m = \{[(a_4 g + a_3)g + a_2]g + a_1\}g + a_0.$$

Beispiel. Die im System der Basis $g = 8$ geschriebene Zahl $m = 73256$ soll dekadisch geschrieben werden. Es ist

$$\begin{aligned} m &= \{[(7 \cdot 8 + 3)8 + 2]8 + 5\}8 + 6 \\ &= \{[59 \cdot 8 + 2]8 + 5\}8 + 6 \\ &= \{474 \cdot 8 + 5\}8 + 6 = 3797 \cdot 8 + 6 \\ &= 30382. \end{aligned}$$

3. Aufgabe. Eine im System der Basis g geschriebene Zahl im System der Basis g' auszudrücken.

Lösung. Man drücke die Zahl erst im dekadischen System (nach Aufgabe 2) und dann das Resultat im System der Basis g' (nach Aufgabe 1) aus.

Beispiel. Es sei α die Ziffer für 10, β diejenige für 11 und $9\alpha 1\beta 2$ eine im System der Basis 12 geschriebene Zahl. Wie wird dieselbe im System der Basis 7 ausgedrückt werden?

Es ist

$$\begin{aligned} & \{[(9.12 + \alpha)12 + 1]12 + \beta\}12 + 2 \\ &= \{[118.12 + 1]12 + \beta\}12 + 2 \\ &= \{1417.12 + 11\}12 + 2 = 17\,015.12 + 2 = 204\,182. \end{aligned}$$

Weiter ergibt sich

$$\begin{array}{rcl} 204\,182 : 7 & = & 29\,168, \text{ Rest } 6, \\ 29\,168 : 7 & = & 4\,166, \quad " \quad 6, \\ 4\,166 : 7 & = & 595, \quad " \quad 1, \\ 595 : 7 & = & 85, \quad " \quad 0, \\ 85 : 7 & = & 12, \quad " \quad 1, \\ 12 : 7 & = & 1, \quad " \quad 5. \end{array}$$

Wir erhalten somit

$$\begin{aligned} 9\alpha 1\beta 2 \text{ (dodekadisch)} &= 204\,182 \text{ (dekadisch)} \\ &= 1510166 \text{ (heptadisch)}. \end{aligned}$$

Man kann die Zahl auch direkt aus dem dodekadischen System in das heptadische überführen. Der Gang der Rechnung würde dann folgender sein:

$$\begin{aligned} 12.15 + 13 &= 226; 226.15 + 1 = 4063; \\ 4063.15 + 14 &= 100\,415; 100\,415.15 + 2 = 1\,510\,166. \end{aligned}$$

§. 2.

Das dyadische System.

Das System mit der Basis 2, welches nur die Ziffern 0, 1 benutzt, ist von besonderer Wichtigkeit und würde den Vorzug vor allen anderen Systemen verdienen, wenn es nicht schon für mäßig große Zahlen allzu große Ausdrücke erforderte. Das Rechnen ist in diesem System am einfachsten. Bei der Addition hat man nämlich nur die beiden Fälle $1 + 0 = 1$, $1 + 1 = 10$,

bei der Subtraktion nur $1 - 0 = 1$, $10 - 1 = 1$, bei der Multiplikation $0.1 = 0$, $1.1 = 1$ zu merken, und jede Division ist, da jeder Partialquotient höchstens 1 beträgt, von vornherein nichts als eine Reihe von Subtraktionen. Ähnlich verhält es sich mit der Ausziehung der Quadratwurzel u. s. w. Um zu zeigen, wie sich das Rechnen in diesem System gestalten würde, lasse ich für die angeführten Rechnungsarten je ein Beispiel folgen.

Addition:

dekadisch	dyadisch
47	101 111
13	1 101
<u>60</u>	<u>111 100</u>

Subtraktion:

dekadisch	dyadisch
47	101 111
13	1 101
<u>34</u>	<u>100 010</u>

Multiplikation:

dekadisch	dyadisch
47.13	101111.1101
141	101111
<u>611</u>	<u>101111</u>
	1001100011

Division:

dekadisch	dyadisch
47 : 13 = 3	101111 : 1101 = 11
<u>8</u>	<u>1101</u>
	10101
	<u>1101</u>
	1000

Ausziehung der Quadratwurzel:

$$\begin{array}{r}
 \sqrt{57,45} = 75 \\
 145 \overline{) 845} \\
 \underline{725} \\
 120
 \end{array}
 \qquad
 \begin{array}{r}
 \sqrt{101101110001} = 1001011 \\
 10001 \overline{) 11001} \\
 \underline{10001} \\
 10001 \\
 1001001 \\
 \underline{1001001} \\
 1001011 \\
 \underline{1001011} \\
 1001011 \\
 \underline{1001011} \\
 111000
 \end{array}$$

Will man eine dekadisch geschriebene Zahl im dyadischen System ausdrücken, so hat man nach §. 1, Aufgabe 1 zu verfahren. Bei großen Zahlen kürzt man (Legendre, *Théorie des Nombres*, 3^{te} Ed. I, p. 246) die Rechnung vorteilhaft dadurch ab, daß man gleich durch $64 = 1000000$, den Quotienten wieder durch 64 u. s. w. dividiert. Um z. B. 73539 dyadisch zu schreiben, rechnet man

$$\begin{aligned}
 73539 : 64 &= 1149, \text{ Rest } 3; \\
 1149 : 64 &= 17, \text{ Rest } 61.
 \end{aligned}$$

Es ist also

$$73539 = 17 \cdot 64^2 + 61 \cdot 64 + 3$$

oder, da

$$17 = 10001, \quad 61 = 111101, \quad 3 = 11$$

ist,

$$73539 = 10001111101000011.$$

Vergl. auch Leibniz, *Mathem. Schriften*, herausgegeben von C. J. Gerhardt VII, S. 223 bis 234.

Anwendung. Die Zauberkarten. — Man schreibe alle Zahlen bis zu einer gewissen Grenze im dyadischen System, also $1=1$, $2=10$, $3=11$, $4=100$, $5=101$, $6=110$, $7=111$ u. s. w. Darauf schreibe man diejenigen dieser Zahlen, die auf der letzten Stelle (rechts) 1 enthalten, also 1, 3, 5, 7, ... auf ein Blatt, weiter die Zahlen, welche auf der vorletzten Stelle 1 enthalten, also 2, 3, 6, 7, u. s. w. auf ein zweites Blatt, alle Zahlen, welche auf der drittletzten Stelle 1 enthalten, also 4, 5, 6, 7, u. s. w. auf ein drittes Blatt, und fahre so fort, bis alle Zahlen des betrachteten Gebietes, so oft es geht, untergebracht sind. Dann ist offenbar jede dieser Zahlen m gleich der Summe der Zahlen, welche den

ersten Platz auf den Blättern einnehmen, auf denen m sich vorfindet. Dies ist die Erklärung der „Zauberkarten“ unserer Spielbücher.

§. 3.

Formen der Zahlen.

Wenn man eine Zahl durch 2 dividiert, so ergibt sich als Rest entweder 0 oder 1. Im ersten Falle ist die Zahl von der Form $2n$ oder eine gerade Zahl, im zweiten von der Form $2n + 1$ oder eine ungerade Zahl.

Bei der Division durch 3 sind drei Reste möglich, nämlich 0, 1 und 2. Jede Zahl gehört also einer der drei Formen $3n$, $3n + 1$, $3n + 2$ an. Eine Zahl der dritten dieser Formen ist z. B. $17 = 3 \cdot 5 + 2$. Wenn man hier den Quotienten 5 um eine Einheit vergrößert, so ist als Rest -1 zu nehmen, $17 = 3 \cdot 6 - 1$, und so kann stets ein Rest, der mehr als die Hälfte des Divisors beträgt, durch einen negativen Rest ersetzt werden, dessen absoluter Wert kleiner als die Hälfte des Divisors ist. Nur darf man dann nicht vergessen, den Quotienten um 1 zu vergrößern. In Beziehung auf den Divisor 3 sind danach die drei Formen $3n$, $3n \pm 1$ vorhanden.

Für den Divisor 4 ergeben sich ebenso die vier Formen $4n$, $4n \pm 1$, $4n + 2$, allgemein für den Divisor k die Formen

$$kn + r,$$

wo r jede der Zahlen $0, 1, 2, \dots, k - 1$ sein kann, und wo jede Zahl r , die größer als $\frac{k}{2}$ ist, durch ihre negativ genommene Ergänzung zu k , deren absoluter Wert dann kleiner als $\frac{k}{2}$ sein wird, ersetzt werden kann.

§. 4.

Primzahlen und zusammengesetzte Zahlen.

Wenn eine ganze Zahl a durch eine andere ganze Zahl b ohne Rest teilbar ist, so nennt man b einen Divisor von a . Ergiebt die Division von a durch b den Quotienten c , so ist auch c ein

Divisor von a , da $a:c=b$ ist. Man nennt dann b und c komplementäre Divisoren von a . So sind 3 und 4 komplementäre Divisoren von 12, ebenso 2 und 6.

Nun ist offenbar jede Zahl a durch sich selbst und ebenso durch die Einheit teilbar, hat also die komplementären Divisoren 1 und a . Diese Divisoren werden uneigentliche genannt, im Gegensatz zu den eigentlichen, die zwischen 1 und a liegen. Die eigentlichen Divisoren von 12 z. B. sind 2, 3, 4, 6. Eine Zahl, welche keine eigentlichen Divisoren besitzt, heisst eine Primzahl. Eine Zahl mit eigentlichen Divisoren heisst zusammengesetzt. Eine Primzahl ist z. B. 11, da keine Zahl ausser 1 und 11 selbst in 11 aufgeht. Eine zusammengesetzte Zahl ist 12, da nicht blofs 1 und 12, sondern auch 2, 3, 4, 6 in 12 aufgehen.

Anmerkung. Euklid VII, Def. 11 und 13 nennt die Primzahl *πρῶτος ἀριθμός*, die zusammengesetzte Zahl *σύνθετος ἀριθμός*. Nikomachus von Gerasa (*Εἰσαγωγή* I, Kap. 11 und 12) gebraucht die Ausdrücke *πρῶτος καὶ ἀσύνθετος ἀριθμός* und *δεύτερος καὶ σύνθετος ἀριθμός*.

§. 5.

Sätze über die Formen von Primzahlen.

Jede ungerade Primzahl ist von einer der beiden Formen $4n \pm 1$.

Jede Primzahl, die gröfser als 3 ist, ist von einer der beiden Formen $6n \pm 1$ ¹⁾.

Jede ungerade Primzahl ist von einer der vier Formen $8n \pm 1$, $8n \pm 3$.

Jede Primzahl, die gröfser als 3 ist, ist von einer der vier Formen $12n \pm 1$, $12n \pm 5$.

Das Quadrat jeder Primzahl, die gröfser als 3 ist, hat die Form $24n + 1$.

¹⁾ Nach G. Vacca (Bibl. math. 3. Folge II, S. 149) ist dieser Satz schon von Bungus (Numerorum Mysteria etc. Bergomi 1559, S. 399) ausgesprochen; später teilt ihn Leibniz in einem Briefe vom Februar 1678 dem Herausgeber des Journal des Savans mit (Math. Schriften, herausgegeben von C. J. Gerhardt VII, S. 120).

Jede Zahl von der Form $4n - 1$ ist entweder eine Primzahl oder durch eine ungerade Anzahl von Primzahlen der Form $4n - 1$ teilbar.

Jede Zahl $6n - 1$ ist entweder eine Primzahl oder durch eine ungerade Anzahl von Primzahlen der Form $6n - 1$ teilbar.

Der Beweis dieser Sätze, denen sich noch andere ähnliche anreihen lassen, sei dem Leser zur Übung empfohlen.

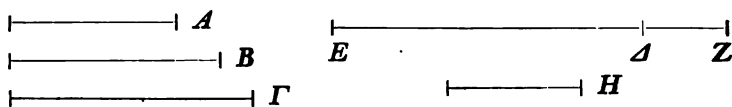
§. 6.

Anzahl der Primzahlen.

Wer zuerst die wichtige Wahrheit gefunden hat, daß es unendlich viele Primzahlen giebt, wissen wir nicht. Aber schon Euklid hat IX, 20 einen strengen Beweis des Satzes gegeben. Als Probe von der Darstellungsweise dieses großen Mathematikers lasse ich den Beweis in wörtlicher Übersetzung hier folgen:

„Die Anzahl der Primzahlen ist größer als jede vorgelegte Menge derselben.

„Die vorgelegten Primzahlen seien A, B, Γ . Ich behaupte, daß es mehr Primzahlen als A, B, Γ giebt.



„Man nehme die kleinste der durch A, B, Γ teilbaren Zahlen; diese sei $\angle E$, und es werde $\angle E$ die Einheit $\angle Z$ hinzugefügt. Dann ist (die Summe) EZ entweder eine Primzahl, oder sie ist es nicht. Es sei EZ zunächst eine Primzahl. Dann sind die Primzahlen A, B, Γ, EZ gefunden, und deren Menge ist größer als die der Zahlen A, B, Γ .

„Weiter sei die Zahl EZ keine Primzahl; dann ist sie durch irgend eine Primzahl teilbar. Sie sei teilbar durch die Primzahl H . Dann behaupte ich, daß H mit keiner der Zahlen A, B, Γ identisch ist. Wäre nämlich H mit einer der Zahlen A, B, Γ identisch, so müßte, da A, B, Γ in $\angle E$ aufgehen, auch H in $\angle E$ aufgehen. H geht aber auch in EZ auf. Folglich wird H , obwohl sie eine Zahl¹⁾ ist, auch in dem der Einheit

¹⁾ D. h. von 1 verschieden. Bei den Griechen wurde die Einheit nicht als Zahl angesehen ($\eta \mu\acute{o}\nu\alpha\varsigma \circ\upsilon\kappa \epsilon\sigma\tau\iota\nu \acute{\alpha}\rho\iota\theta\mu\acute{o}\varsigma$).

gleichen Rest $\mathcal{A}Z$ aufgehen, und das ist widersinnig. H ist also mit keiner der Zahlen $\mathcal{A}$, B , Γ identisch. H ist aber der Voraussetzung nach eine Primzahl. Folglich sind Primzahlen $\mathcal{A}$, B , Γ , H in größerer Menge gefunden, als die Anzahl der vorgelegten Primzahlen $\mathcal{A}$, B , Γ beträgt, und dafs dies möglich sei, war zu zeigen.“

Anmerkung. Die kleinste Zahl, welche durch die als vorhanden angenommenen Primzahlen 2, 3, 5, 7, ... p teilbar ist, ist — wie wir später sehen werden — das Produkt derselben. Wird dieses Produkt, nachdem es um 1 vermehrt ist, mit $\mathcal{A}$ bezeichnet, also

$$\mathcal{A} = 2.3.5.7.11 \dots p + 1$$

gesetzt, so ergibt die Rechnung, dafs für die Werte $p = 2, 3, 5, 7, 11$ $\mathcal{A}$ selbst eine Primzahl und beziehungsweise gleich 3, 7, 31, 211, 2311 ist; dagegen ist für $p = 13, 17, 19, 23$

$$\mathcal{A} = 59.509, 19.97.277, 347.27953, 317.703763.$$

2. Beweis des Satzes, dafs es unendlich viele Primzahlen giebt (Euler, *Introductio in Analysin Infinitorum* I, p. 225). Bekanntlich ist

$$\frac{1}{1 - \frac{1}{2}} = 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \dots \text{ in inf.},$$

$$\frac{1}{1 - \frac{1}{3}} = 1 + \frac{1}{3} + \frac{1}{9} + \frac{1}{27} + \dots \text{ in inf.},$$

$$\frac{1}{1 - \frac{1}{5}} = 1 + \frac{1}{5} + \frac{1}{25} + \frac{1}{125} + \dots \text{ in inf.}$$

.

Daraus erhält man durch Multiplikation

$$\frac{1}{1 - \frac{1}{2}} \cdot \frac{1}{1 - \frac{1}{3}} \dots = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \dots$$

In dieser Gleichung enthält die linke Seite so viele Faktoren, als es Primzahlen giebt, die rechte Seite die reziproken Werte aller ganzen Zahlen, da jede Zahl entweder selbst eine Primzahl ist oder — und zwar nur auf eine Weise — durch Multiplikation aus Primzahlen entsteht. Nun läfst sich leicht beweisen, dafs die

rechte Seite ∞ ist¹⁾). Folglich muß auch die Anzahl der Faktoren der linken Seite jede Grenze überschreiten, d. h. es giebt unendlich viele Primzahlen.

1. Zusatz. Es giebt unendlich viele Primzahlen der Form $4n - 1$.

2. Zusatz. Es giebt unendlich viele Primzahlen der Form $6n - 1$.

Die Beweise sind dem oben gegebenen 1. Beweise ganz ähnlich; nur hat man A im ersten Satze durch $(2^a \cdot 3 \cdot 5 \dots p) - 1$, im zweiten durch $(2 \cdot 3 \cdot 5 \dots p) - 1$ zu ersetzen.

3. Zusatz. Es giebt unendlich viele Primzahlen jeder der beiden Formen $4n + 1$, $8n + 5$.

Der Beweis kann hier nicht geführt werden.

Anmerkung I. Alle diese Sätze sind spezielle Fälle des von Lejeune Dirichlet (Abhandlungen der Berliner Akademie 1837 = Werke Bd. I, S. 313) bewiesenen Satzes:

Jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Faktor sind, enthält unendlich viele Primzahlen.

Anmerkung II. Hierher gehört auch der von Tschescheff bewiesene Satz: Wenn $2a > 7$ ist, so liegt zwischen a und $2a - 2$ wenigstens eine Primzahl (Serret, Handbuch der höheren Algebra, deutsch von G. Wertheim, Bd. II, S. 193).

Noch unbewiesen sind folgende Sätze:

1. Es giebt unendlich viele Paare von Primzahlen, deren Differenz 2 ist.
2. Jede gerade Zahl ist die Summe zweier Primzahlen (Christian Goldbach).
3. Jede Primzahl der Form $4n - 1$ ist gleich $p + 2q$, wo p und q Primzahlen der Form $4n + 1$ sind (Lagrange, Oeuvres T. III, p. 795).

¹⁾ Dieselbe ist nämlich:

$$> 1 + \frac{1}{2} + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}\right) + \dots,$$

d. i.

$$> 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \dots \text{ in inf.,}$$

also $= \infty$.

§. 7.

Ermittlung der Primzahlen.

Um aus der Reihe der Zahlen die zusammengesetzten auszuscheiden, so daß nur die Primzahlen zurückbleiben, wendet man ein von Eratosthenes (275 bis 194 v. Chr.) herrührendes Verfahren an, welches unter dem Namen „Sieb (*κόσκινον*) des Eratosthenes“ bekannt ist, und über welches Nikomachos von Gerasa in seiner „*Ἀριθμητικὴ εἰσαγωγή*“ I, 13 berichtet. Dasselbe besteht im folgenden:

Da 2 die einzige gerade Primzahl ist, so hat man nur die ungeraden Zahlen von 3 an niederzuschreiben:

3, 5, 7, 9, 11, 13, 15, 17, ...

Man streicht nun jede dritte Zahl hinter der 3 durch, also die dritte, d. i. 9, die sechste, d. i. 15, die neunte, d. i. 21, u. s. w. Auf diese Weise werden alle Vielfachen von 3 entfernt.

Darauf geht man zur nächsten Zahl, d. i. 5 über und streicht hinter derselben jede fünfte Zahl durch, also die fünfte, zehnte, fünfzehnte, u. s. w., ohne Rücksicht darauf, ob sie schon durch einen früheren Strich ausgeschieden ist oder nicht. Auf diese Weise werden alle Vielfachen von 5 beseitigt.

Weiter entfernt man alle Vielfachen von 7, indem man hinter der 7 jede siebente Zahl durchstreicht, und fährt so fort, indem man beim Abzählen und Durchstreichen die bereits durchstrichenen Zahlen den nicht durchstrichenen gleich achtet, ohne freilich — denn das wäre zwecklos — eine durchstrichene Zahl als Ausgangspunkt einer neuen Aussiebung zu benutzen. Schließlich bleiben nur die Primzahlen übrig, alle (ungeraden) zusammengesetzten Zahlen sind entfernt worden.

Die letzte Primzahl, die man als Ausgangspunkt einer Abzählung in der dargelegten Weise zu benutzen hat, um alle Primzahlen unterhalb einer gegebenen Grenze a zu erhalten, liefert der folgende, schon von Leonardo Pisano (Scritti ed. Boncompagni T. I, p. 38) angewandte, auch Fermat (Oeuvres II, p. 177) bekannte Satz, den Legendre (Théorie des Nombres 3^{ième} Ed. I, p. 5) bewiesen hat:

„Eine Zahl N ist sicherlich eine Primzahl, wenn sie durch keine der Primzahlen teilbar ist, die $< \sqrt{N}$ sind.“

Beweis. Wir nehmen an, N sei durch eine Primzahl $p > \sqrt{N}$ teilbar, und bezeichnen den Quotienten der Division von N durch p mit P , setzen also $N = pP$ voraus. Dann würde $P = \frac{N}{p}$, also $P < \frac{N}{\sqrt{N}}$, d. i. $P < \sqrt{N}$ sein. Die Zahl N wäre also durch eine Zahl $P < \sqrt{N}$ und um so mehr durch eine Primzahl $< \sqrt{N}$ teilbar, was der Voraussetzung widerspricht.

Die letzte Zahl, von der aus man abzuzählen hat, um alle unterhalb a liegenden Primzahlen zu erhalten, ist somit die größte Primzahl, die $\leq \sqrt{a}$ ist.

Beispiel. Da $\sqrt{150} = 12, \dots$ und 11 die größte Primzahl unterhalb 12 ist, so hat man, um alle (ungeraden) Primzahlen unterhalb 150 zu erhalten, in der oben dargelegten Weise nur mit 3, 5, 7, 11 zu verfahren. Es ergibt sich:

3,	5,	7,	~~9,~~	11,	13,	~~15,~~	17,	19,	~~21,~~
23,	~~25,~~	~~27,~~	29,	31,	~~33,~~	~~35,~~	37,	~~39,~~	41,
43,	~~45,~~	47,	~~49,~~	~~51,~~	53,	~~55,~~	~~57,~~	59,	61,
~~63,~~	~~65,~~	67,	~~69,~~	71,	73,	~~75,~~	~~77,~~	79,	~~81,~~
83,	~~85,~~	~~87,~~	89,	~~91,~~	~~93,~~	~~95,~~	97,	~~99,~~	101,
103,	~~105,~~	107,	109,	~~111,~~	113,	~~115,~~	~~117,~~	~~119,~~	~~121,~~
~~123,~~	~~125,~~	127,	~~129,~~	131,	~~133,~~	~~135,~~	137,	139,	~~141,~~
~~143,~~	~~145,~~	~~147,~~	149,						

Unterhalb 150 liegen also die 34 ungeraden Primzahlen:

3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149.

Wie man sieht, ist die Ermittlung der Primzahlen für ein größeres Gebiet, etwa für die erste Million, theoretisch zwar sehr einfach, thatsächlich aber ungemein zeitraubend. Ich lasse daher die Titel der Werke folgen, welche ausgedehnte Tabellen der Primzahlen (und zugleich die kleinsten Divisoren der zusammengesetzten ungeraden Zahlen, sofern diese nicht durch 3 oder 5 teilbar sind) enthalten:

1. Burckhardt, Table des diviseurs pour tous les nombres du 1., 2. et 3. million. Paris 1814—1817 (geht bis 3 036 000).

2. Glaisher, Factor-table for the 4th, the 5th and the 6th million. London, 1879—1883.

3. Dase, Faktorentafel für alle Zahlen der siebenten, achten und neunten Million. Hamburg, 1862—1865.

In betreff der Korrektheit dieser Tafeln siehe die Arbeit von Gram in den Acta mathematica XVII.

§. 8.

Darstellung der Primzahlen durch Polynome.

Lehrsatz. Das Polynom mit ganzen Koeffizienten

$$f(x) = ax^m + bx^n + \dots + c$$

kann nicht für alle Werte von x Primzahlen darstellen.

Beweis. Es sei ξ ein Wert von x , für welchen $f(x)$ eine Primzahl p ist, also

$$f(\xi) = a\xi^m + b\xi^n + \dots + c = p.$$

Dann ist

$$f(\xi + p) = a(\xi + p)^m + b(\xi + p)^n + \dots + c,$$

also nach dem binomischen Satze

$$f(\xi + p) = p + P,$$

wo

$$\begin{aligned} P = & am\xi^{m-1}p + \dots + ap^m \\ & + bn\xi^{n-1}p + \dots + bp^n \\ & + \dots \end{aligned}$$

eine durch p teilbare Zahl ist. Das Polynom $f(x)$ stellt also für $x = \xi + p$ eine durch p teilbare Zahl dar, und da dieselbe von p verschieden ist, so muß sie zusammengesetzt sein.

1. Anmerkung. Einige Polynome sind bemerkenswert durch die Menge der Primzahlen, die sie darstellen. Setzt man z. B. der Reihe nach $x = 0, 1, 2, 3, \dots$, so liefert

$x^2 + x + 11$	bis $x = 9$	$2x^2 + 2x + 19$	bis $x = 17$
$x^2 + x + 17$	" $x = 15$	$3x^2 + 3x + 23$	" $x = 21$
$x^2 + x + 41$	" $x = 39$	$4x^2 + 7$	" $x = 6$
$2x^2 + 11$	" $x = 10$	$5x^2 + 5x + 13$	" $x = 11$
$2x^2 + 29$	" $x = 28$	$6x^2 + 6x + 31$	" $x = 28$
$2x^2 + 2x + 7$	" $x = 5$		

nur Primzahlen. Vergl. Euler, *Commentationes arithmeticae collectae* I, p. 584 und Legendre, *Théorie des nombres* I, p. 332.

2. Anmerkung. Fermat war der Meinung (*Varia Opera math.*, p. 162 = *Oeuvres* T. II, p. 206), der Ausdruck $2^{(2^n)} + 1$ stelle für jede ganze Zahl n eine Primzahl dar; er fügt hinzu, daß er einen Beweis des Satzes nicht gefunden habe. Nun sind zwar $2^{(2^0)} + 1 = 3$, $2^{(2^1)} + 1 = 5$, $2^{(2^2)} + 1 = 17$, $2^{(2^3)} + 1 = 257$, $2^{(2^4)} + 1 = 65537$ Primzahlen, aber schon $2^{(2^5)} + 1 = 4294967297$ ist, wie Euler (*Commentationes arithmeticae collectae* I, p. 356) ermittelt hat, zusammengesetzt, nämlich gleich 641.6700417 . (Vergl. §. 100, Beispiel I.)

§. 9.

Primzahlen gleicher Differenz.

Lehrsatz. Wenn drei Primzahlen eine arithmetische Reihe bilden, so muß die Differenz derselben durch $2.3 = 6$ teilbar sein. Eine Ausnahme macht nur der Fall, in welchem 3 eine der Zahlen ist (*Waring, Meditationes Algebraicae*, p. 379. Siehe auch Lagrange, *Oeuvres* T. III, p. 434).

Beweis. Die Primzahlen gleicher Differenz d seien

$$(1) \quad p - d, \quad p, \quad p + d;$$

darin ist p von einer der beiden Formen $6m \pm 1$, und damit $p - d$ und $p + d$ ungerade seien, muß d als gerade vorausgesetzt werden. d könnte danach eine der drei Formen $6n \pm 2$, $6n$ haben, und es soll gezeigt werden, daß die beiden ersten Formen unmöglich sind.

Wäre erstens $d = 6n + 2$, so würde sich für die Zahlen (1), je nachdem $p = 6m + 1$ oder $= 6m - 1$ vorausgesetzt wird,

$$6(m - n) - 1, \quad 6m + 1, \quad 6(m + n) + 3$$

oder

$$6(m - n) - 3, \quad 6m - 1, \quad 6(m + n) + 1$$

ergeben. Im ersten Falle ist $6(m + n) + 3$ immer eine zusammengesetzte Zahl, im zweiten Falle ist es $6(m - n) - 3$, wofern nicht $m - n = 1$, also $6(m - n) - 3 = 3$ ist. Die Differenz d kann also nicht die Form $6n + 2$ haben, wofern nicht die erste Zahl 3 ist; in diesem Falle sind die Zahlen (1)

$$3, \quad 6n + 5, \quad 12n + 7.$$

Wäre zweitens $d = 6n - 2$, so würde sich für die Zahlen (1), je nachdem $p = 6m + 1$ oder $= 6m - 1$ vorausgesetzt wird,

$$6(m - n) + 3, \quad 6m + 1, \quad 6(m + n) - 1$$

oder

$$6(m - n) + 1, \quad 6m - 1, \quad 6(m + n) - 3$$

ergeben. Im zweiten Falle ist $6(m + n) - 3$ immer zusammengesetzt, im ersteren ist es $6(m - n) + 3$, wofern nicht $m = n$ ist, also die Zahlen (1)

$$3, \quad 6n + 1, \quad 12n - 1$$

sind. Die Differenz kann also, diesen Fall abgerechnet, auch nicht $6n - 2$ sein; es bleibt für dieselbe also nur die Form $6n$ übrig, und für diese sind die Zahlen (1), je nachdem $p = 6m \pm 1$ ist,

$$6(m - n) \pm 1, \quad 6m \pm 1, \quad 6(m + n) \pm 1.$$

Der Fall $p = 3$ war durch die Annahme $p = 6m \pm 1$ von vornherein ausgeschlossen.

Ähnlich lassen sich folgende Sätze beweisen:

Wenn fünf Primzahlen eine arithmetische Reihe bilden, so muß die Differenz derselben durch $2.3.5 = 30$ teilbar sein, wofern nicht 5 selbst eine der Zahlen ist.

Wenn sieben Primzahlen eine arithmetische Reihe bilden, so muß die Differenz derselben durch $2.3.5.7 = 210$ teilbar sein, wofern nicht 7 selbst eine der Zahlen ist. U. s. w.

§. 10.

Darstellung der Zahlen als Summen aufeinander folgender Zahlen.

Lehrsatz. Jede Zahl, die nicht eine Potenz von 2 ist, kann als Summe mehrerer aufeinander folgender Zahlen dargestellt werden.

Beweis. Wir setzen die Richtigkeit des Satzes für eine Zahl m , die gerade oder ungerade sein mag, voraus und beweisen, daß er dann auch für $2m$ besteht. Da er nun für jede ungerade Zahl gilt, insofern als $2n + 1 = n + (n + 1)$ ist, so ist seine Gültigkeit für alle Zahlen, die einen ungeraden Divisor zulassen, bewiesen.

Es sei zunächst m die Summe einer ungeraden Anzahl $2k + 1$ aufeinander folgender Zahlen, etwa

$$m = (n - k) + (n - k + 1) + \dots + n + (n + 1) + \dots + (n + k),$$

so ist

$$2m = (2n - k) + (2n - k + 1) + \dots + 2n + (2n + 1) + \dots + (2n + k).$$

So z. B. folgt aus $6 = 1 + 2 + 3$, daß $12 = 3 + 4 + 5$,
 $24 = 7 + 8 + 9$, $48 = 15 + 16 + 17$, u. s. w. ist.

Ebenso ergibt sich aus

$$20 = 2 + 3 + 4 + 5 + 6$$

der Reihe nach

$$40 = 6 + 7 + 8 + 9 + 10$$

$$80 = 14 + 15 + 16 + 17 + 18$$

$$\dots \dots \dots$$

Ist dagegen m die Summe einer geraden Anzahl $2k$ aufeinander folgender Zahlen

$$m = (n - k - 1) + \dots + (n - 1) + n + (n + 1) + \dots + (n + k),$$

so erhält man leicht

$$2m = (n - 2k - 1) + \dots + (n - 1) + n + (n + 1) + \dots + (n + 2k).$$

Aus $50 = 11 + 12 + 13 + 14$ folgt z. B. $100 = 9 + 10 + 11 + 12 + 13 + 14 + 15 + 16$.

§. 11. Darstellung der Zahlen als Differenz zweier Quadrate. 17

In diesem Falle kann es vorkommen, daß die erste Zahl Null wird, oder daß negative Glieder auftreten, die dann aber gegen die symmetrisch stehenden positiven von gleichem absoluten Betrage wegfallen. So z. B. folgt aus $3 = 1 + 2$

$$6 = 0 + 1 + 2 + 3 = 1 + 2 + 3,$$

und aus

$$36 = 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8$$

folgt, daß

$$72 = (-3) + (-2) + (-1) + 0 + 1 + \dots + 8 + 9 + 10 \\ + 11 + 12$$

oder

$$72 = 4 + 5 + 6 + \dots + 12$$

ist.

Der Satz ist also für jede Zahl $2^a k$, wo k eine ungerade Zahl bezeichnet, bewiesen.

Es ist noch zu zeigen, daß sich keine Potenz von 2 als Summe aufeinander folgender Zahlen darstellen läßt. Setzt man die Formeln für $2m$ als gültig voraus, so ergeben sich daraus auch diejenigen für m ; wenn also irgend eine Potenz 2^a die Summe aufeinander folgender Zahlen wäre, so müßte es auch die vorhergehende Potenz 2^{a-1} , weiter 2^{a-2} , endlich die Zahl 2 selbst sein, was nicht der Fall ist.

Anmerkung. Bei der Ausführung der Zerlegung wird man oft gut thun, nicht erst auf den in der Zahl enthaltenen größten ungeraden Faktor zurückzugehen. Handelt es sich z. B. um die Zahl 84, so könnte man, da $84 = 4 \cdot 21$ und $21 = 10 + 11$ ist,

$$84 = 7 + 8 + 9 + 10 + 11 + 12 + 13 + 14$$

schreiben. Statt dessen wird man berücksichtigen, daß 84 durch 3 teilbar und allgemein $3a = (a-1) + a + (a+1)$ ist. Man erhält dann einfacher $84 = 27 + 28 + 29$. Ebenso ist $93 = 30 + 31 + 32$.

§. 11.

Darstellung der Zahlen als Differenz zweier Quadrate.

I. Lehrsatz. Jede ungerade Primzahl p ist nur auf eine Weise als Differenz zweier Quadrate darzustellen.

Beweis. Wenn

$$p = x^2 - y^2 = (x - y)(x + y)$$

ist, so muß

$$x - y = 1, \quad x + y = p$$

sein; es ergibt sich also nur die eine Lösung

$$x = \frac{p+1}{2}, \quad y = \frac{p-1}{2},$$

so daß

$$p = \left(\frac{p+1}{2}\right)^2 - \left(\frac{p-1}{2}\right)^2$$

ist.

2. Lehrsatz (Umkehrung). Eine ungerade Zahl p ist eine Primzahl, wenn sie nur auf eine Weise als Differenz zweier Quadrate dargestellt werden kann.

Beweis. Wäre $p = p_1 \cdot p_2$, wo p_1, p_2 ungerade Zahlen bezeichnen mögen, von denen jede > 1 ist, so würden sich die beiden Zerlegungen

$$p = \left(\frac{p_1 + p_2}{2}\right)^2 - \left(\frac{p_1 - p_2}{2}\right)^2$$

$$p = \left(\frac{p_1 p_2 + 1}{2}\right)^2 - \left(\frac{p_1 p_2 - 1}{2}\right)^2$$

ergeben.

Anwendung. Um zu bestimmen, ob eine ungerade Zahl p eine Primzahl sei oder nicht, addiert man zu derselben der Reihe nach alle Quadratzahlen

$$1, 4, 9, \dots, \left(\frac{p-1}{2}\right)^2.$$

Stellt sich heraus, daß nur eine der erhaltenen Summen eine Quadratzahl ist, so ist p eine Primzahl, im entgegengesetzten Falle ist p zusammengesetzt. Es ist nun immer

$$p + \left(\frac{p-1}{2}\right)^2 = \left(\frac{p+1}{2}\right)^2.$$

Wenn also p von irgend einer Quadratzahl außer der letzten, d. i. $\left(\frac{p-1}{2}\right)^2$, zu einem Quadrat ergänzt wird, so ist p zusammengesetzt.

Beispiel. Da $9991 + 3^2 = 100^2$ ist, so ist 9991 eine zusammengesetzte Zahl, nämlich $(100 - 3)(100 + 3)$, d. i. $97 \cdot 103$.

Frage. Welche geraden Zahlen lassen sich als Differenz zweier Quadrate schreiben, und welche nicht?

Anmerkung. In einem Briefe aus dem Jahre 1643, der in Bd. II, S. 256 der neuen Ausgabe seiner Werke zum ersten Male veröffentlicht worden ist, lehrt Fermat an einem Beispiel eine ungerade Zahl in zwei Faktoren zu zerlegen. Im folgenden soll sein Verfahren allgemein dargestellt werden:

Die vorgelegte Zahl sei m . Ferner habe man gefunden $a < \sqrt{m} < a + 1$, und zwar $m = a^2 + r$. Wir bilden die Zahl $2a + 1 - r$. Ist dieselbe eine Quadratzahl n^2 , so ist $r = 2a + 1 - n^2$, also

$$m = a^2 + 2a + 1 - n^2 = (a + 1 - n)(a + 1 + n),$$

und die Zerlegung von m in Faktoren ist vollbracht. Wenn dagegen $2a + 1 - r$ keine Quadratzahl ist, so addieren wir zu $2a + 1 - r$ der Reihe nach die Summe der arithmetischen Reihe

$$2a + 3, 2a + 5, \dots, 2a + (2n - 1),$$

und zwar brechen wir bei dem ersten Gliede $2a + (2n - 1)$ ab, welches eine Quadratzahl s^2 liefert. Es ist dann

$$2a + 1 - r + (2a + 3) + (2a + 5) + \dots + [2a + (2n - 1)] = s^2,$$

d. h.

$$2na + n^2 - r = s^2,$$

folglich

$$m = a^2 + r = a^2 + 2na + n^2 - s^2 = (a + n + s)(a + n - s).$$

Fermat findet auf diese Weise

$$2027651281 = 46061.44021.$$

Es kommt also darauf an, für jede Zahl m die Werte von n und s zu finden, was die Anwendung einer Tabelle der Quadratzahlen erfordert. Die Rechnung schließt um so schneller ab, je kleiner die Differenz der Faktoren von m ist.

§. 12.

Zusammengesetzte Zahlen und Zerlegung derselben in Faktoren.

„Jede zusammengesetzte Zahl ist durch irgend eine Primzahl teilbar.

„Die zusammengesetzte Zahl sei A . Ich behaupte, daß A durch irgend eine Primzahl teilbar ist.

„Da die Zahl A zusammengesetzt ist, so ist sie durch eine Zahl teilbar. Diese Zahl sei B . Wenn dann B eine Primzahl ist, so ist die Behauptung bewiesen. Ist aber B eine zusammengesetzte Zahl, so wird diese durch eine andere Zahl teilbar sein. Diese Zahl sei Γ . Da nun Γ in B und B in A aufgeht, so geht auch Γ in A auf. Wenn nun Γ eine Primzahl ist, so ist die Behauptung bewiesen. Ist aber Γ eine zusammengesetzte Zahl, so wird sie durch eine andere Zahl teilbar sein. Durch Fortsetzung dieses Schlussverfahrens wird eine Primzahl gefunden werden, welche (in die vorhergehende Zahl und somit auch in A) aufgeht. Denn sonst würden unzählige Zahlen in A aufgehen, von denen jede kleiner als die vorhergehende wäre, und das ist bei ganzen Zahlen unmöglich. Man wird also eine Primzahl finden, durch welche die nächst vorhergehende Zahl und somit auch A teilbar ist. Folglich ist jede zusammengesetzte Zahl durch irgend eine Primzahl teilbar, und das war zu beweisen.“ (Euklid VII, 31.)

Aus diesem Satze geht hervor, daß sich jede zusammengesetzte Zahl als Produkt von lauter Primzahlen darstellen läßt.

Wir wollen jetzt zeigen, daß diese Zerlegung einer zusammengesetzten Zahl in Primzahlen nur auf eine Weise möglich ist, d. h. daß Zerlegungen, die etwa auf verschiedenen Wegen erhalten sind, identisch sein müssen.

1. Hilfssatz. Das Produkt zweier ganzen positiven Zahlen, von denen jede kleiner als eine Primzahl p ist, ist durch p nicht teilbar (Gauss, Disquisitiones 13).

Beweis. Es sei p eine Primzahl und a eine positive Zahl, die kleiner als p ist. Dann giebt es keine positive Zahl b , die kleiner als p ist, von der Beschaffenheit, daß das Produkt ab durch p teilbar sei.

Dies zu beweisen, nehmen wir an, es gebe mehrere Zahlen $b, c, d, \dots$, die sämtlich kleiner als p und so beschaffen sind, daß jedes der Produkte $ab, ac, ad, \dots$ durch p teilbar sei. Die kleinste der Zahlen $b, c, d, \dots$ sei b , so daß also keine Zahl, die kleiner als b ist, durch Multiplikation mit a ein durch p teilbares Produkt liefert. Nun muß offenbar $b > 1$ sein; denn für $b = 1$ wäre $ab = a$, also nach Voraussetzung $< p$ und daher

durch p nicht teilbar. Wenn wir jetzt die Primzahl p durch $b < p$ dividieren, so kann die Division nicht aufgehen, sondern wir werden einen Quotienten m und einen Rest $b' < b$ erhalten, so daß

$$p = bm + b', \text{ also } p - bm = b'$$

ist. Daraus folgt

$$ap - abm = ab'.$$

Nun ist sowohl ap , als auch (nach Voraussetzung) abm durch p teilbar; folglich muß p auch in ab' aufgehen. Danach gehört auch die Zahl b' zu den Zahlen $b, c, d, \dots$, obwohl sie kleiner als die kleinste derselben ist. Es giebt also keine Zahl $b < p$ von der Beschaffenheit, daß ab durch p teilbar sei.

2. Hilfssatz. Wenn keine der beiden Zahlen a und b durch die Primzahl p teilbar ist, so ist auch das Produkt ab durch p nicht teilbar (l. c. 14).

Beweis. Wir dividieren jede der beiden Zahlen a, b durch p und nennen die erhaltenen Quotienten q, q' , die erhaltenen Reste, die von Null verschieden und $< p$ sein werden, α und β . Dann ist

$$a = qp + \alpha, \quad b = q'p + \beta,$$

also

$$ab = (qq'p + \alpha q' + \beta q)p + \alpha\beta.$$

Wäre nun ab durch p teilbar, so müßte es auch $\alpha\beta$ sein, und das ist nach dem 1. Hilfssatze unmöglich.

Zusatz. Wenn keine der Zahlen $a, b, c, d, \dots$ durch die Primzahl p teilbar ist, so ist auch das Produkt $abcd \dots$ durch p nicht teilbar (l. c. 15).

Beweis. Nach dem 2. Hilfssatze ist ab durch p nicht teilbar, folglich (nach demselben Satze) auch nicht $ab.c = abc$, u. s. w.

Lehrsatz. Jede zusammengesetzte Zahl kann nur auf eine Weise in Primzahlfactoren zerlegt werden.

Beweis. Angenommen, es hätten sich für eine Zahl N die beiden Zerlegungen ergeben:

$$N = aa'a'' \dots \text{ und } N = bb'b'' \dots,$$

wo $a, a', \dots, b, b', \dots$ Primzahlen bezeichnen. Dann ist

$$(1) \quad aa'a'' \dots = bb'b'' \dots$$

Da die Primzahl a in der linken Seite von (1) aufgeht, so muß auch die rechte Seite durch a teilbar sein. Das ist nach dem

vorhergehenden Zusatz unmöglich, wofern nicht die rechte Seite einen Faktor enthält, der gleich a ist. Dieser Faktor sei b . Dann fallen die Primzahlen a und b durch Division fort, und (1) geht über in

$$(2) \quad a' a'' \dots = b' b'' \dots$$

Auf diese Gleichung können wir dasselbe Schlussverfahren anwenden, dem wir die Gleichung (1) unterworfen haben. Wir finden auf diese Weise, daß jedem Faktor der linken Seite von (1) ein Faktor der rechten Seite gleich ist, und daß beide Seiten gleich viel Faktoren enthalten. Die beiden Zerlegungen stimmen also — abgesehen von der Reihenfolge der Faktoren, die bekanntlich für die GröÙe des Produktes gleichgültig ist — vollständig überein.

Jede zusammengesetzte Zahl N ist also nur auf eine Weise als Produkt von Primzahlen darzustellen. Werden dann noch die etwa vorhandenen gleichen Primzahlen zu Primzahlpotenzen vereinigt, so ergibt sich für N der Ausdruck

$$N = a^\alpha b^\beta c^\gamma \dots,$$

wo $a, b, c, \dots$ ungleiche Primzahlen, $\alpha, \beta, \gamma, \dots$ ganze positive Zahlen bezeichnen.

Beispiele:

$$\text{I.} \quad 720 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 2^4 \cdot 3^2 \cdot 5,$$

$$\text{II.} \quad 18900 = 2^2 \cdot 3^3 \cdot 5^2 \cdot 7.$$

Aufgabe. n aufeinander folgende zusammengesetzte Zahlen zu finden.

Lösung. Man wähle n beliebige aufeinander folgende Zahlen:

$$a, a + 1, a + 2, \dots, a + n - 1,$$

von denen die kleinste, d. i. a , größer als 1 ist. Nimmt man dann eine Zahl A , die durch jede dieser n Zahlen teilbar ist, so sind

$$A + a, A + a + 1, A + a + 2, \dots, A + a + n - 1$$

n aufeinander folgende zusammengesetzte Zahlen. Da nämlich A durch a teilbar ist, so ist es auch $A + a$; da weiter A durch $a + 1$ teilbar ist, so ist es auch $A + a + 1$, u. s. w.

Beispiel. Da 420 durch jede der fünf aufeinander folgenden Zahlen

$$3, 4, 5, 6, 7$$

teilbar ist, so sind

$$423, 424, 425, 426, 427$$

fünf aufeinander folgende zusammengesetzte Zahlen, und zwar ist die erste durch 3 teilbar, die zweite durch 4, u. s. w.

§. 13.

Divisoren einer Zahl. Anzahl, Summe und Produkt derselben.

Wir nehmen an, es sei

$$m = a^{\alpha} b^{\beta} c^{\gamma} \dots$$

wo $a, b, c, \dots$ ungleiche Primzahlen, $\alpha, \beta, \gamma, \dots$ ganze positive Zahlen sind, und stellen uns die Aufgabe, die sämtlichen Divisoren von m zu bilden.

Da die Zahl m den Faktor a^a enthält, so ist sie durch die $a+1$ Zahlen

$$(1) \quad 1, a, a^2, \dots, a^{\alpha}$$

teilbar. Weiter gehen in m , des Faktors b^β wegen, die Zahlen auf, die entstehen, wenn man jede der Zahlen (1) mit jeder der Zahlen $b, b^2, \dots, b^\beta$ multipliziert. Auf diese Weise erhält man $(\alpha + 1)\beta$ neue Divisoren von m , nämlich

$$(2) \quad \begin{cases} b, & ab, & a^2b, & \dots, & a^\alpha b \\ b^2, & ab^2, & a^2b^2, & \dots, & a^\alpha b^2 \\ \dots & \dots & \dots & \dots & \dots \\ b^\beta, & ab^\beta, & a^2b^\beta, & \dots, & a^\alpha b^\beta. \end{cases}$$

Man hat dann im ganzen $\alpha + 1 + (\alpha + 1)\beta = (\alpha + 1)(\beta + 1)$ Divisoren. Dazu kommen drittens, wegen des Faktors c^γ , alle diejenigen Zahlen, die man erhält, wenn man jede der Zahlen (1) und (2) mit jeder der γ Zahlen $c, c^2, \dots, c^\gamma$ multipliziert. Da auf diese Weise $(\alpha + 1)(\beta + 1)\gamma$ neue Divisoren entstehen, so liefern die Faktoren $a^\alpha, b^\beta, c^\gamma$ im ganzen

$$(\alpha+1)(\beta+1) + (\alpha+1)(\beta+1)\gamma = (\alpha+1)(\beta+1)(\gamma+1)$$

Divisoren von m . So fortfahrend erkennt man, daß die Zahl
 $m = a^{\alpha} b^{\beta} c^{\gamma} \dots k^{\kappa}$

$$(\alpha + 1)(\beta + 1)(\gamma + 1) \dots (x + 1)$$

Divisoren hat. Dieselben sind offenbar die Glieder des Produkts

$$(1+a+a^2+\dots+a^x)(1+b+\dots+b^y)\dots(1+k+\dots+k^x),$$

ihre Summe beträgt somit

$$\frac{a^{\alpha+1}-1}{a-1} \cdot \frac{b^{\beta+1}-1}{b-1} \cdot \dots \cdot \frac{k^{\kappa+1}-1}{k-1}.$$

Beispiel. Die Zahl $360 = 2^3 \cdot 3^2 \cdot 5$ hat $(3+1)(2+1)(1+1) = 24$ Divisoren; es sind dies die Glieder des Produkts

$$(1+2+4+8)(1+3+9)(1+5),$$

also die Zahlen

$$\begin{array}{l} 1, 2, 4, 8; \quad 3, 6, 12, 24; \quad 9, 18, 36, 72; \\ 5, 10, 20, 40; \quad 15, 30, 60, 120; \quad 45, 90, 180, 360. \end{array}$$

Ihre Summe beträgt

$$\frac{2^4-1}{2-1} \cdot \frac{3^3-1}{3-1} \cdot \frac{5^2-1}{5-1} = \frac{15}{1} \cdot \frac{26}{2} \cdot \frac{24}{4} = 15 \cdot 13 \cdot 6 = 1170.$$

Lehrsatz. Bezeichnet μ die Anzahl der Divisoren einer Zahl m , so ist das Produkt derselben $m^{\frac{1}{2}\mu}$.

Beweis. Wenn m keine Quadratzahl ist, so lassen sich die Divisoren in Gruppen von je zweien so zusammenstellen, daß das Produkt der Glieder jeder Gruppe gleich m ist. Da sich nun im ganzen $\frac{\mu}{2}$ Gruppen ergeben, so ist das Produkt aller Divisoren $m^{\frac{1}{2}\mu}$.

Ist dagegen m eine Quadratzahl, $m = a^{2\alpha} b^{2\beta} \dots k^{2\kappa}$, also die Anzahl der Divisoren eine ungerade Zahl $\mu = 2\nu + 1$, so können wir vorläufig den Divisor $\sqrt{m} = a^{\alpha} \dots k^{\kappa}$ ausscheiden und die übrigen Divisoren in Gruppen von je zweien in der Weise ordnen, daß wieder die Glieder jeder Gruppe das Produkt m haben. Da ν solcher Gruppen vorhanden sind, so ergibt sich als Gesamtprodukt m^{ν} , und wenn wir diese Zahl mit dem letzten Divisor $\sqrt{m}$ multiplizieren, so erhalten wir als Produkt aller Divisoren $m^{\nu + \frac{1}{2}}$, d. i. $m^{\frac{1}{2}\mu}$.

Beispiel. $360 = 2^3 \cdot 3^2 \cdot 5$ hat $4 \cdot 3 \cdot 2 = 24$ Divisoren, deren Summe 1170 und deren Produkt 360^{12} ist.

Aufgaben. I. Welches ist die kleinste Zahl, die 24 Divisoren hat?

Lösung. Da $24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 4 = 3 \cdot 8 = 2 \cdot 2 \cdot 6 = 2 \cdot 12 = 4 \cdot 6 = 1 \cdot 24$ ist, so hat jede Zahl jeder der sieben

Formen $abcd^2$, ab^2c^3 , a^2b^7 , abc^5 , ab^{11} , a^3b^5 , a^{23} , wo a , b , c , d ungleiche Primzahlen bedeuten, 24 Divisoren. Die kleinste Zahl der ersten Form ist $2^2 \cdot 3 \cdot 5 \cdot 7 = 420$, die der zweiten $2^3 \cdot 3^2 \cdot 5 = 360$, die der dritten $2^7 \cdot 3^2 = 1152$, die der vierten $2^5 \cdot 3 \cdot 5 = 480$, die der fünften $2^{11} \cdot 3 = 6144$, die der sechsten $2^5 \cdot 3^3 = 864$, die der siebenten $2^{23} = 8388608$, also die kleinste von allen 360.

II. Welche Zahl ist gleich dem Produkt ihrer Divisoren (die Zahl selbst ausgeschlossen)?

Lösung. Es soll

$$m = \frac{m^{\frac{1}{2}\mu}}{m} = m^{\frac{1}{2}\mu - 1},$$

also

$$\frac{1}{2}\mu - 1 = 1,$$

d. h. $\mu = 4$ sein. Die Zahl muß also vier Divisoren haben, oder, da $4 = 1 \cdot 4 = 2 \cdot 2$ ist, von einer der beiden Formen

$$p^3, \quad p \cdot q$$

sein, wo p , q Primzahlen bedeuten.

III. Beweise, daß eine Zahl mit einer ungeraden Anzahl von Divisoren eine Quadratzahl ist.

IV. Beweise, daß eine Zahl, für welche die Anzahl der Divisoren eine Primzahl q ist, die Form p^{q-1} haben muß, wo p ebenfalls eine Primzahl bezeichnet.

V. Die Divisorensumme von 751530^3 zu bestimmen. Es ist;

$$751530^3 = 2^3 \cdot 3^3 \cdot 5^3 \cdot 13^3 \cdot 41^3 \cdot 47^3,$$

$$2^4 - 1 = 15 = 3 \cdot 5,$$

$$\frac{3^4 - 1}{2} = 40 = 2^3 \cdot 5,$$

$$\frac{5^4 - 1}{4} = 156 = 2^2 \cdot 3 \cdot 13,$$

$$\frac{13^4 - 1}{12} = 2380 = 2^3 \cdot 5 \cdot 7 \cdot 17,$$

$$\frac{41^4 - 1}{40} = 70644 = 2^2 \cdot 3 \cdot 7 \cdot 29^2,$$

$$\frac{47^4 - 1}{46} = 106080 = 2^5 \cdot 3 \cdot 5 \cdot 13 \cdot 17,$$

also die gesuchte Divisorensumme

$$2^{14} \cdot 3^4 \cdot 5^4 \cdot 7^2 \cdot 13^2 \cdot 17^2 \cdot 29^2,$$

d. i. das Quadrat von

$$2^7 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 13 \cdot 17 \cdot 29.$$

VI. Beweise folgenden Satz: Wenn $2^a + 1$ eine Primzahl ist, so beträgt die Zahl $2^{a-1}(2^a + 1)$ zwei Einheiten mehr als die Summe ihrer Divisoren (die Zahl selbst natürlich ausgeschlossen).

VII. Entwickelt man (durch Division) den Ausdruck

$$\frac{x}{1-x} + \frac{x^2}{1-x^2} + \frac{x^3}{1-x^3} + \dots$$

nach steigenden Potenzen von x , so erhält man die Reihe

$$x + 2x^2 + 2x^3 + 3x^4 + 2x^5 + 4x^6 + 2x^7 + \dots$$

Es soll bewiesen werden, daß der Koeffizient jedes Gliedes gleich der Anzahl der Divisoren seines Exponenten ist, daß also im besonderen jedes Glied, dessen Exponent eine Primzahl ist, den Koeffizienten 2 hat (Lambert, s. Lacroix, traité du calcul diff. et du calc. int. III, p. 466).

VIII. Die Zahl $m = a^\alpha b^\beta c^\gamma \dots$, in welcher $a, b, c \dots$ ungleiche Primzahlen, $\alpha, \beta, \gamma, \dots$ ganze positive Zahlen bezeichnen, ist die r^{te} Potenz einer ganzen Zahl k , wenn jeder der Exponenten $\alpha, \beta, \gamma, \dots$ durch r teilbar ist.

1. Anmerkung. Fermat¹⁾ hat (Varia Opera math., p. 188 = Oeuvres II, p. 332) im Jahre 1657 dem Wallis und den übrigen englischen Mathematikern die beiden Aufgaben gestellt:

Einen Kubus zu finden, dessen Divisorensumme ein Quadrat ist, wie z. B. 343, für welche Zahl man $1 + 7 + 49 + 343 = 400 = 20^2$ hat.

Ein Quadrat zu finden, dessen Divisorensumme ein Kubus ist.

Wallis behandelt die Sache Opera, Bd. II, p. 511 ff. und p. 824 ff. und stellt zugleich die Gegenaufgabe:

Zwei Quadrate von gleicher Divisorensumme zu finden, wie es z. B. 25 und 16 sind, da $1 + 5 + 25 = 1 + 2 + 4 + 8 + 16 = 31$ ist.

¹⁾ Näheres darüber findet man in der Arbeit von G. Wertheim: Pierre Fermats Streit mit John Wallis (Abhandlungen zur Geschichte der Mathematik, Bd. IX).

Die Lösung dieser und ähnlicher Aufgaben setzt die Herstellung einer Tabelle voraus, in der für jede Zahl die zugehörige Divisorensumme angegeben ist. Man kann sich dabei nach dem oben für die Divisorensumme hergeleiteten Ausdruck auf die Primzahlen und die Potenzen derselben beschränken, und was die letzteren betrifft, so erhält man offenbar die Divisorensumme von a^{n+1} , indem man a^{n+1} zu derjenigen von a^n addiert.

2. Anmerkung. Eine merkwürdige Formel zur Berechnung der Divisorensumme einer Zahl hat Euler gefunden und nach vielen Bemühungen mittels Betrachtungen, die das Gebiet der Elementarmathematik überschreiten, bewiesen (*Observatio de summis divisorum, Commentationes arithmeticae collectae, I, p. 146 ff.* S. auch Bachmann, *Analytische Zahlentheorie, S. 25*).

§. 14.

Vollkommene Zahlen.

Eine Zahl heißt vollkommen, wenn sie der Summe ihrer Divisoren, die Zahl selbst ausgeschlossen, gleich ist, mit anderen Worten, wenn die Divisorensumme das Doppelte der Zahl ist. Beträgt dagegen die Divisorensumme mehr oder weniger als das Doppelte der Zahl, so heißt die Zahl im ersten Falle überschiefsend, im zweiten mangelhaft. (Von den vollkommenen Zahlen spricht schon Euklid [IX, 36], von den überschiefsenden und mangelhaften erst Nikomachos von Gerasa, I, 14—16.)

Ungerade vollkommene Zahlen sind zur Zeit nicht bekannt. Hinsichtlich der geraden gelten folgende Sätze:

1. **Lehrsatz.** Eine gerade vollkommene Zahl muß von der Form $2^a(2^{a+1} - 1)$ sein, wo $2^{a+1} - 1$ eine Primzahl ist.

Beweis. Es sei

$$m = 2^a p^b q^c \dots$$

eine vollkommene Zahl, also nach der Definition

$$(1+2+2^2+\dots+2^a)(1+p+p^2+\dots+p^b)(1+q+\dots+q^c)\dots \\ = 2^{a+1} p^b q^c \dots,$$

oder

$$\begin{aligned} (1+p+\dots+p^\beta)(1+q+\dots+q^\gamma)\dots &= \frac{2^{\alpha+1} p^\beta q^\gamma \dots}{2^{\alpha+1} - 1} \\ &= \frac{(2^{\alpha+1} - 1) p^\beta q^\gamma \dots + p^\beta q^\gamma \dots}{2^{\alpha+1} - 1} = p^\beta q^\gamma \dots + \frac{p^\beta q^\gamma \dots}{2^{\alpha+1} - 1}. \end{aligned}$$

Da nun

$$(1+p+\dots)(1+q+\dots)\dots$$

eine ganze Zahl ist, so muß auch

$$\frac{p^\beta q^\gamma \dots}{2^{\alpha+1} - 1}$$

eine ganze Zahl sein, und zwar eine Zahl, welche keine anderen Primzahlen als $p, q, \dots$ enthalten kann. Die rechte Seite der Gleichung

$$(1+p+\dots+p^\beta)(1+q+\dots+q^\gamma)\dots = p^\beta q^\gamma \dots + \frac{p^\beta q^\gamma \dots}{2^{\alpha+1} - 1}$$

enthält also zwei Glieder; dasselbe muß folglich mit der linken Seite der Fall sein, es muß also

$$\beta = 1, \quad \gamma = \delta = \dots = 0$$

vorausgesetzt werden, d. h. es ist

$$m = 2^\alpha \cdot p,$$

wo p eine Primzahl bezeichnet, deren Form jetzt bestimmt werden soll.

Nach der Definition der vollkommenen Zahlen ist

$$(2^{\alpha+1} - 1)(1 + p) = 2^{\alpha+1} p = (2^{\alpha+1} - 1)p + p;$$

daraus ergibt sich durch Division mit $2^{\alpha+1} - 1$

$$1 + p = p + \frac{p}{2^{\alpha+1} - 1},$$

und damit

$$\frac{p}{2^{\alpha+1} - 1} = 1$$

sei, ist

$$p = 2^{\alpha+1} - 1$$

anzunehmen.

2. Lehrsatz. Wenn $2^{\alpha+1} - 1$ eine Primzahl ist, so ist $2^\alpha(2^{\alpha+1} - 1)$ eine vollkommene Zahl (Euklid, IX, 36).

Beweis. Die Divisorensumme der Zahl $2^\alpha(2^{\alpha+1} - 1)$ ist nach dem Früheren, da der zweite Faktor eine Primzahl ist, gleich

$$\frac{2^{\alpha+1} - 1}{2 - 1} (2^{\alpha+1} - 1 + 1) = 2^{\alpha+1} \cdot (2^{\alpha+1} - 1),$$

also gleich dem Doppelten der Zahl.

Anmerkungen. I. Die Division von $(2^{mn} - 1) : (2^m - 1)$ ergibt als Quotienten $1 + 2^m + 2^{2m} + \dots + 2^{(n-1)m}$. Daher ist $2^{mn} - 1$ sowohl durch $2^m - 1$, als auch durch $2^n - 1$ teilbar, und $2^{\alpha+1} - 1$ kann nur dann eine Primzahl sein, wenn $\alpha + 1$ eine Primzahl ist. Man darf aber nicht umgekehrt sagen, daß für jede Primzahl $\alpha + 1$ auch $2^{\alpha+1} - 1$ eine Primzahl sei. Die folgende, aus E. Lucas, *Théorie des Nombres*, p. 375 entnommene Tabelle giebt die gegenwärtig bekannten Primzahlen p , für welche $2^p - 1$ eine zusammengesetzte Zahl ist; neben jede dieser Zahlen p ist der kleinste Divisor d gestellt, den $2^p - 1$ zuläßt.

p	d	p	d	p	d
11	23	59	179 951	179	359
23	47	73	439	191	383
29	233	79	2 687	211	15 193
37	223	83	167	223	18 287
41	13 367	97	11 447	233	1 399
43	431	113	3 391	239	479
47	2 351	131	263	251	503
53	6 361	151	18 121		
p	d	p	d	p	d

Die ersten acht gegenwärtig bekannten vollkommenen Zahlen giebt die folgende Tabelle:

p	$2^p - 1$	$2^p - 1$	$2^{p-1} (2^p - 1)$
2	2	3	6
3	4	7	28
5	16	31	496
7	64	127	8 128
13	4 096	8 191	33 550 336
17	65 536	131 071	8 589 869 056
19	262 144	524 287	137 438 691 328
31	1 073 741 824	2 147 483 647	2 305 643 008 139 952 128

Eine neunte, dem Werte $p = 61$ entsprechende vollkommene Zahl hat Paul Seelhoff ermittelt.

II. Die letzte Ziffer einer (dekadisch geschriebenen) vollkommenen Zahl ist 6 oder 8¹⁾; denn es sind die Endungen von:

2^{p-1}	2	4	8	6	2	..
2^p	4	8	6	2	4	..
$2^p - 1$	3	7	5	1	3	..
$2^{p-1}(2^p - 1)$	6	8	—	6	6	..

III. Jede vollkommene Zahl, mit Ausnahme von 6, giebt bei der Division durch 9 den Rest 1. (Der Satz ist zuerst 1510 von Charles de Bouvelles ausgesprochen und 1603 von Pietro Antonio Cataldi bewiesen.) $2^p - 1$ und 2^{p-1} geben nämlich bei der Division durch 9 für die Werte von $p - 1 = 0, 1, 2, \dots$ die in der folgenden Tabelle angegebenen Reste:

$p - 1$	1	2	3	4	5	6	7	8	9	..
$2^p - 1$. . .	3	7	6	4	0	1	3	7	6	..
2^{p-1}	2	4	8	7	5	1	2	4	8	..

Da $2^p - 1$ eine Primzahl sein soll, so fallen die Formen $9k + 6$, $9k$, $9k + 3$ weg. Jede Primzahl $2^p - 1$, mit Ausnahme der Zahl 3, ist also von einer der Formen

$$9k + 7, \quad 9k + 4, \quad 9k + 1,$$

denen beziehungsweise die Formen

$$9l + 4, \quad 9l + 7, \quad 9l + 1$$

von 2^{p-1} entsprechen, und da das Produkt zweier Zahlen der einander entsprechenden Formen offenbar bei der Division durch 9 den Rest 1 ergibt, so ist der Satz bewiesen.

IV. Im dyadischen System ist eine vollkommene Zahl von der Form

$$\underbrace{111 \dots 1}_{n+1} \underbrace{000 \dots 0}_n,$$

so z. B. ist $6 = 110$, $28 = 11100$, $496 = 111110000$, u. s. w.

¹⁾ Diese Thatsache war schon dem Nikomachus von Gerasa bekannt. *Ἀριθμητικὴ Εἰσαγωγή*, Ausgabe von R. Hoche, S. 40.

V. Aus der Betrachtung der Tabelle

p	1	2	3	4	5	6	7	8	9	10	11	..
$2^p - 1$	1	3	7	15	31	63	127	255	511	1023	2047	..

entnimmt Fermat (*Varia Opera math.*, p. 177 = *Oeuvres II*, p. 198) folgende Sätze, die er die Grundlage für die Ermittlung der vollkommenen Zahlen nennt, und die er, wie er sagt, nicht ohne Mühe bewiesen habe:

1. Wenn p eine zusammengesetzte Zahl ist, so ist auch $2^p - 1$ zusammengesetzt.

2. Wenn p eine Primzahl ist, so ist $2^p - 2$ immer durch $2p$ teilbar.

3. Wenn p eine Primzahl ist, so ist $2^p - 1$ nur durch Primzahlen von der Form $2kp + 1$, wo k eine ganze Zahl bedeutet, teilbar. (S. §. 99, Lehrsatz II.)

Der erste dieser Sätze ist oben in der ersten Anmerkung bewiesen.

Der zweite Satz ist ein specieller Fall des „Fermat'schen Satzes“, der uns später beschäftigen wird.

Der dritte Satz verringert erheblich die Anzahl der Divisionen, die man vorzunehmen hat, um zu finden, ob $2^p - 1$ eine Primzahl sei oder nicht. Um z. B. $2^{11} - 1 = 2047$ zu prüfen, hat man die Division nur mit den Primzahlen der Form $22k + 1$, die kleiner als $\sqrt{2047} = 45, \dots$ sind, also nur mit der einen Zahl 23 zu versuchen; es ergibt sich, daß $2047 = 23 \cdot 89$ ist. Ebenso findet man, daß $8191 = 2^{13} - 1$ eine Primzahl ist, da diese Zahl weder durch 53, noch durch 79 teilbar ist.

VL Statt Zahlen zu suchen, bei denen die jedesmalige Divisorensumme das Doppelte der Zahl beträgt (vollkommene Zahlen), kann man auch nach Zahlen fragen, bei denen die Divisorensumme das Dreifache oder das Vierfache u. s. w. der Zahl ist. Mit dieser schon von Fermat (*Varia Opera math.*, p. 178 = *Oeuvres II*, p. 248) in Angriff genommenen allgemeineren Aufgabe hat sich besonders (für specielle Fälle) Legendre (*Théorie des nombres II*, p. 146 ff.) beschäftigt.

§. 15.

Befreundete Zahlen.

Zwei Zahlen heißen befreundet, wenn jede derselben der Summe der Divisoren der andern, mit Ausschluss der Zahl selbst, gleich ist, oder, was auf dasselbe hinausläuft, wenn die ganze Divisorensumme einer jeden gleich der Summe der beiden Zahlen ist. Von dieser Art sind z. B. $284 = 2^2 \cdot 71$ und $220 = 2^2 \cdot 5 \cdot 11$; denn es ist

$$1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284$$

und

$$1 + 2 + 4 + 71 + 142 = 220,$$

oder die Summe der Divisoren von 284 ist $7 \cdot 72 = 504$, und die von 220 ist $7 \cdot 6 \cdot 12 = 504 = 284 + 220$.

Anmerkung. Mit den befreundeten Zahlen haben sich schon die alten Pythagoräer beschäftigt (s. Cantor, Geschichte der Mathematik, I, S. 156 und 691); die erste Regel zur Bildung derselben hat der arabische Gelehrte Tábit ibn Kurra (826—901) gegeben. Dieselbe lautet:

„Wenn $p = 3 \cdot 2^n - 1$, $q = 3 \cdot 2^{n-1} - 1$ und $r = 3^2 \cdot 2^{2n-1} - 1$ gleichzeitig Primzahlen sind, so sind

$$A = 2^n p q \text{ und } B = 2^n r$$

befreundet“. Le Lasseur hat nach Edouard Lucas, Théorie des Nombres, I, p. 381 die Werte von p, q, r für $n = 1, 2, 3, \dots, 35$ geprüft und gefunden, daß nur den drei Werten $n = 2, 4, 7$ befreundete Zahlen entsprechen. Die von Bernard Frenicle de Bessy dem Claude Mylon mitgeteilte Regel zur Bildung befreundeter Zahlen (Oeuvres de Huygens, II, p. 26) ist mit der von Tábit ibn Kurra gegebenen im Grunde identisch. Am meisten hat sich Euler mit dem Gegenstande beschäftigt (Opuscula varii argumenti, II, p. 23 ff. = Commentationes arithm. collectae, I, p. 102 ff.), auch Legendre behandelt denselben (Théorie des nombres, II, p. 148).

§. 16.

Der größte gemeinschaftliche Divisor von Zahlen.
Relative Primzahlen.

Wenn wir die Divisoren einer Zahl mit denjenigen einer zweiten Zahl vergleichen, so sind zwei Fälle möglich: Die Zahlen

haben entweder (außer der Einheit) einen oder mehrere Divisoren gemeinschaftlich, oder es sind keine gemeinschaftlichen Divisoren vorhanden. Im letzteren Falle, wenn die beiden Zahlen also nur den Divisor 1 gemeinschaftlich haben, nennt man sie teilerfremd oder prim zu einander oder relative Primzahlen. Im ersteren Falle erhebt sich die Frage, wie der grösste gemeinschaftliche Divisor der Zahlen gefunden werden könne.

So z. B. hat

12	die Divisoren	1, 2, 3, 4, 6, 12;
30	"	1, 2, 3, 5, 6, 10, 15, 30;
175	"	1, 5, 7, 25, 35, 175.

Die Zahlen 12 und 30 haben also die Divisoren 2, 3, 6 gemeinschaftlich; der grösste derselben ist 6. Die Zahlen 30 und 175 haben nur den Divisor 5 gemeinschaftlich. Die Zahlen 12 und 175 sind relative Primzahlen, da keiner der Divisoren von 12 zugleich ein Divisor von 175 ist.

Man kann auch mehr als zwei Zahlen daraufhin betrachten, ob sie Divisoren (außer 1) sämtlich gemeinsam haben oder nicht. Die oben betrachteten drei Zahlen 12, 30, 175 sind teilerfremd, die Zahlen 12, 30, 42, 66 haben den grössten gemeinschaftlichen Divisor 6.

Wenn jede der vorgelegten Zahlen in ihre Primzahlpotenzen zerlegt ist, so macht die Beantwortung der Frage, ob dieselben teilerfremd seien, und welches im entgegengesetzten Falle ihr grösster gemeinschaftlicher Divisor sei, keine Schwierigkeit. Die Zahlen sind teilerfremd, wenn keine Primzahl da ist, die in allen Zerlegungen vorkommt. Wenn die Zahlen nicht teilerfremd sind, so findet man ihren grössten gemeinschaftlichen Divisor auf folgende Weise: Man nimmt sämtliche den vorgelegten Zahlen gemeinschaftliche Primfaktoren, giebt jedem den kleinsten Exponenten, den er in einer der Zahlen hat, und multipliziert die so erhaltenen Potenzen. So z. B. haben die Zahlen

$$2100 = 2^2 \cdot 3 \cdot 5^2 \cdot 7, \quad 8820 = 2^2 \cdot 3^2 \cdot 5 \cdot 7^2, \quad 360 = 2^3 \cdot 3^2 \cdot 5$$

den grössten gemeinschaftlichen Divisor $2^2 \cdot 3 \cdot 5 = 60$.

Sehen wir jetzt, wie zu verfahren ist, wenn die vorgelegten Zahlen nicht erst in ihre Primzahlpotenzen zerlegt werden sollen.

1. Aufgabe. Den grössten gemeinschaftlichen Divisor zweier Zahlen a und $b < a$ zu ermitteln (Euklid VII, 2).

Wenn die Zahl b in a aufgeht, so ist sie, da sie auch in sich selbst aufgeht, ein gemeinschaftlicher Divisor von a und b . Sie ist aber auch der grösste gemeinschaftliche Divisor, da keine grössere Zahl als b in b aufgehen kann.

Wir nehmen jetzt an, b gehe nicht in a auf. Wir dividieren dann a durch b . Die Division ergebe den Quotienten q und den Rest $r < b$, so daß $a = bq + r$ ist. Aus dieser Gleichung erkennt man sofort, daß der grösste gemeinschaftliche Divisor von a und b mit demjenigen von b und r identisch ist. Weiter dividieren wir b durch r ; der Quotient sei q_1 , der Rest r_1 . Dann wird $r_1 < r$ und der grösste gemeinschaftliche Divisor von b und r , also auch derjenige von a und b mit dem von r und r_1 identisch sein. In dieser Weise fahren wir fort, bis der Rest Null erscheint, und da die Reste immer kleiner werden, so muß dies nach einer endlichen Anzahl von Divisionen einmal geschehen. Wir haben dann die Gleichungen

$$\begin{aligned} a &= bq + r \\ b &= r q_1 + r_1 \\ r &= r_1 q_2 + r_2 \\ &\dots \dots \dots \\ r_{m-1} &= r_m q_{m+1} + r_{m+1} \\ r_m &= r_{m+1} q_{m+2}, \end{aligned}$$

aus deren letzter hervorgeht, daß der grösste gemeinschaftliche Divisor von r_m und r_{m+1} , also auch derjenige aller vorhergehenden Zahlenpaare r_{m-1} und r_m , ..., r und r_1 , b und r , a und b der zuletzt als Divisor benutzte Rest r_{m+1} ist.

Folgerung: Wenn eine Zahl in zwei gegebenen Zahlen aufgeht, so geht sie auch in dem grössten gemeinschaftlichen Divisor derselben auf.

2. Aufgabe. Den grössten gemeinschaftlichen Divisor mehrerer Zahlen $a, b, c, \dots$ zu bestimmen (Euklid VII, 3).

Man bestimme den grössten gemeinschaftlichen Divisor d der beiden Zahlen a, b . Wenn dann erstens d in c aufgeht, so ist die Zahl d , weil sie auch in a und b aufgeht, ein gemeinschaftlicher Divisor von a, b, c und zwar — wie wir jetzt beweisen wollen — der grösste gemeinschaftliche Divisor dieser drei Zahlen. Hätten dieselben nämlich einen gemeinschaftlichen Divisor e , der $> d$ wäre, so würde die Zahl e , weil sie in a und b aufgeht, auch in d aufgehen müssen, was wegen $e > d$ unmöglich ist. In

diesem Falle ist also d der grösste gemeinschaftliche Divisor von a, b, c .

Wenn zweitens d in c nicht aufgeht, so läßt sich zunächst zeigen, daß d und c nicht teilerfremd sein können, sobald angenommen wird, daß a, b, c einen gemeinschaftlichen Divisor haben. Dieser muß nämlich, da er in a und b aufgeht, auch in d aufgehen; er geht aber auch in c auf, ist also d und c gemeinschaftlich. Somit können c und d nicht teilerfremd sein. Wir bestimmen jetzt den grössten gemeinschaftlichen Divisor e von c und d . Da nun e in d und d in a, b aufgeht, so wird e ebenfalls in a, b aufgehen. e ist aber auch in c enthalten, folglich ist e ein gemeinschaftlicher Divisor von a, b, c . Es ist noch zu beweisen, daß e der grösste gemeinschaftliche Divisor von a, b, c ist. Ginge $f > e$ in a, b, c auf, so müßte f , als Divisor von a und b , auch in d aufgehen. f ist aber auch in c enthalten, folglich müßte f als gemeinschaftlicher Divisor von d und c auch in e aufgehen, was wegen $f > e$ unmöglich ist. Der grösste gemeinschaftliche Divisor von a, b, c ist also e .

Man erkennt leicht, daß man durch wiederholte Anwendung dieses Verfahrens den grössten gemeinschaftlichen Divisor beliebig vieler gegebenen Zahlen bestimmen kann.

Beispiel. Es soll der grösste gemeinschaftliche Divisor der oben benutzten Zahlen 8820, 2100, 360 bestimmt werden.

Da

$$\begin{aligned} 8820 &= 2100 \cdot 4 + 420, \\ 2100 &= 420 \cdot 5 \end{aligned}$$

ist, so ist 420 der grösste gemeinschaftliche Divisor von 8820 und 2100. Weiter ist

$$420 = 360 \cdot 1 + 60 \quad \text{und} \quad 360 = 60 \cdot 6,$$

also 60 der grösste gemeinschaftliche Divisor der drei vorgelegten Zahlen.

§. 17.

Sätze über relative Primzahlen.

1. Lehrsatz. Wenn a und b relative Primzahlen sind, so geht jeder gemeinschaftliche Divisor von ak und b in k auf.

Beweis. Da a prim zu b ist, so gelangt man bei den in der 1. Aufgabe des §. 16 angegebenen Divisionen zu dem Rest 1, erhält also, wenn man daselbst $r_{m+1} = 1$ annimmt und sodann mit k multipliziert:

$$\begin{aligned} ak &= bqk + rk \\ bk &= r_1q_1k + r_1k \\ &\dots \dots \dots \\ r_{m-1}k &= r_mq_{m+1}k + k. \end{aligned}$$

Die Betrachtung dieser Gleichungen lehrt, daß ein gemeinschaftlicher Divisor von ak und b auch in rk , folglich, weil in b und rk , auch in r_1k , u. s. w., endlich auch in k aufgehen muß.

Ist im besonderen ak durch b teilbar, so muß k durch b teilbar sein.

2. Lehrsatz. Wenn jede der beiden Zahlen a, k prim zu b ist, so ist auch das Produkt ak prim zu b .

Beweis. Ein gemeinschaftlicher Divisor von ak und b müßte nach dem 1. Satz in k aufgehen, während k prim zu b sein soll.

Zusatz. Potenzen relativer Primzahlen sind prim zu einander.

Beweis. Wenn a prim zu b ist, so ist nach dem 2. Satz auch a^2 , daher nach demselben Satz auch a^3 , u. s. w., allgemein a^m prim zu b . Auf dieselbe Weise folgt aus der Annahme, b sei prim zu a^m , daß auch b^2 , b^3 , u. s. w., allgemein b^n prim zu a^m sein muß. a^m und b^n sind also relative Primzahlen.

3. Lehrsatz. Wenn die Summe oder die Differenz zweier irreducibelen Brüche eine ganze Zahl ist, so sind die Nenner der Brüche einander gleich.

Beweis. Es seien a, b, c, d ganze Zahlen, a prim zu b, c prim zu d und zunächst

$$\frac{a}{b} + \frac{c}{d} = e,$$

wo auch e eine ganze Zahl bezeichnet.

Dann ist

$$a = be - \frac{bc}{d},$$

und da c prim zu d ist, so muß d in b aufgehen. Es ist aber auch

$$c = de - \frac{ad}{b},$$

und da a prim zu b ist, so muß b in d aufgehen. Es ist somit $b = d$. Der Beweis ist derselbe für den Fall, daß die Differenz der Brüche eine ganze Zahl ist.

Anwendungen. I. Wir teilen die Peripherie eines Kreises in n gleiche Teile, verbinden einen Teilpunkt mit dem um k Teile entfernten Punkte, diesen mit dem in demselben Sinne wieder um k Teile entfernten Punkte, und fahren so fort, so werden wir schliesslich — nötigenfalls nach mehreren Umläufen — zum Ausgangspunkt zurückgelangen, also ein geschlossenes regelmäßiges Polygon konstruiert haben. Denn da die Anzahl der Ecken eine endliche ist, so muß man schliesslich zu einer schon berührten kommen, und zwar zur Ausgangsecke; denn wäre die von neuem erreichte Ecke eine andere, so wäre von ihr aus ein geschlossenes Polygon gebildet, und ein gleiches müßte dann von der Ausgangsecke aus möglich sein. Das so gebildete Polygon habe m Ecken, wo $m \leq n$ ist.

Wir nehmen nun weiter eine der etwa noch nicht berührten $n - m$ Ecken als neuen Ausgangspunkt und bilden, immer um k Teile weiter gehend, ein zweites Polygon von m Ecken; beide Polygone können keine Ecke gemeinsam haben, da sie sonst vollständig zusammenfallen müßten. Mit den jetzt noch nicht berührten $n - 2m$ Ecken verfahren wir in derselben Weise, bis alle benutzt sind; es werden dann h Polygone von je m Ecken gebildet sein, und da jetzt alle n Ecken, jede einmal, berührt sind, so ist

$$n = mh.$$

Wird weiter die Anzahl der vollständigen Umläufe, die man gemacht hat, um eines der h Polygone zu bilden, mit r bezeichnet, so kann der dabei durchlaufene Weg durch rn ausgedrückt werden. Als zweiter Ausdruck für denselben Weg ergibt sich mk , da das Polygon ein m -Eck ist und der Bogen zwischen je zwei benachbarten Ecken nach Voraussetzung gleich k ist. Es ist also

$$nr = mk,$$

oder, wenn n durch mh ersetzt und sodann durch m dividiert wird, $k = hr$. Aus den beiden Formeln

$$(1) \quad n = hm, \quad (2) \quad k = hr$$

ergibt sich Folgendes:

Die Anzahl h der auf die dargelegte Weise gebildeten Polygone ist gleich dem größten gemeinschaftlichen Divisor von n und k ; es wird im besondern nur ein Polygon entstehen, wenn n und k prim zu einander sind.

II. Beweise folgende Sätze:

1. Dividirt man zwei Zahlen durch ihren größten gemeinschaftlichen Divisor, so sind die Quotienten prim zu einander.

2. Zwei aufeinander folgende Zahlen sind prim zu einander.

3. Die Anzahl der Divisoren einer Potenz ist prim zum Exponenten.

4. In der zuerst von Leonardo Pisano (Scritti, ed. Boncompagni I, p. 283) angewandten Reihe, deren beide ersten Glieder 0, 1 sind, und bei der jedes folgende Glied die Summe der beiden vorhergehenden ist,

$$0, 1, 1, 2, 3, 5, 8, 13, \dots, u_n, u_{n+1}, u_{n+2}, \dots,$$

ist jedes Glied prim zu jedem der beiden folgenden; in derselben Reihe folgen auf ein gerades Glied immer zwei ungerade, auf ein ungerades höchstens ein gerades.

Anmerkung. Mit dieser Reihe haben sich u. a. Albert Girard (s. Oeuvres de Simon Stevin, Leiden 1633, Vol. I, p. 170) und später sehr eingehend Leibniz (Math. Schriften, herausgegeben von C. J. Gerhardt VII, S. 40 ff.) beschäftigt. Ersterer findet, daß $\frac{u_n}{u_{n+1}}$ sich bei wachsendem n der Seite des dem Kreise vom Radius 1 einbeschriebenen regulären Zehneckes nähert. Leibniz giebt noch folgende Eigenschaften der Reihe an:

$$1) \quad u_n - 1 = u_{n-2} + u_{n-3} + \dots + u_0,$$

$$2) \quad u_n \cdot u_{n+3} = u_{n+1} \cdot u_{n+2} \pm 1,$$

$$3) \quad u_{n+1}^2 = u_n \cdot u_{n+2} \pm 1.$$

§. 18.

Das kleinste Vielfache von Zahlen.

Unter dem kleinsten Vielfachen der Zahlen $a, b, c, \dots$ versteht man die kleinste der unendlich vielen Zahlen, die durch jede der Zahlen $a, b, c, \dots$ teilbar sind.

Wenn die Zahlen $a, b, c, \dots$ in ihre Primfaktoren zerlegt sind, so bildet man dieses kleinste Vielfache auf folgende Weise:

Man nimmt jede Primzahl, die in einer der Zahlen $a, b, c, \dots$ vorkommt, giebt ihr den größten Exponenten, den sie in einer derselben hat, und bildet das Produkt der so erhaltenen Potenzen.

Beispiel. Die Zahlen

$$504 = 2^3 \cdot 3^2 \cdot 7, \quad 240 = 2^4 \cdot 3 \cdot 5, \quad 864 = 2^5 \cdot 3^3$$

haben das kleinste Vielfache

$$2^5 \cdot 3^3 \cdot 5 \cdot 7 = 30240.$$

Wir wollen jetzt zeigen, wie man das kleinste Vielfache gegebener Zahlen ermittelt, ohne ihre Primfaktoren zu benutzen (Euklid VII, 34, 35, 36).

1. Aufgabe. Das kleinste Vielfache zweier gegebenen Zahlen a und b zu finden.

Lösung. a und b sind entweder relative Primzahlen, oder sie sind es nicht. Wir setzen erstens voraus, a sei prim zu b , und es sei $ab = c$. Dann ist c ein Vielfaches sowohl von a als auch von b , und wir wollen jetzt beweisen, daß c das kleinste Vielfache dieser beiden Zahlen ist. Gingen a und b in einer Zahl $d < c$ auf und wäre

$$\frac{d}{a} = e, \quad \frac{d}{b} = f,$$

also

$$ae = d, \quad bf = d,$$

so müßte $ae = bf$ sein. Es würde also die Proportion

$$a : b = f : e$$

bestehen, und da a prim zu b ist, so müßte b in e aufgehen. Dann ginge aber auch ab in ae auf, d. i. c in d . Das ist unmöglich, da $d < c$ ist. a und b gehen also in keiner Zahl auf, die kleiner als c ist, oder c ist das kleinste Vielfache von a und b . Das kleinste Vielfache zweier Zahlen, die prim zu einander sind, ist somit das Produkt beider Zahlen.

Zweitens seien a und b nicht prim zu einander. Nehmen wir dann die kleinsten Zahlen f, e , welche dasselbe Verhältniß wie a und b zu einander haben, so daß also $a:b = f:e$ ist, so ergibt sich $ae = bf$, und wenn $ae = c$ ist, so muß auch $bf = c$ sein. Jede der Zahlen a, b geht somit in c auf, oder c

ist ein Vielfaches sowohl von a als auch von b . Wir behaupten nun, daß c das kleinste Vielfache von a und b ist. Gäbe es eine Zahl $d < c$, in die sowohl a als auch b aufginge, und würde

$$\frac{d}{a} = h, \quad \frac{d}{b} = g$$

gesetzt, so hätten wir $ah = d$, $bg = d$, folglich $ah = bg$ oder $a:b = g:h$. Es ist aber auch $a:b = f:e$, folglich müßte $f:e = g:h$ sein, und da f und e die kleinsten Zahlen sein sollen, die sich wie $a:b$ verhalten, so müßte e in h , also auch ae in ah , d. i. c in d aufgehen. Das ist aber unmöglich, da $d < c$ ist. Daher giebt es kein Vielfaches von a und b , das $< c$ wäre, oder c ist das kleinste Vielfache von a und b . Man findet also das kleinste Vielfache zweier Zahlen a und b , die einen grössten gemeinschaftlichen Divisor δ haben, indem man a mit $\frac{b}{\delta}$ oder, was dasselbe ist, b mit $\frac{a}{\delta}$ multipliziert.

Beispiele. Das kleinste Vielfache von 27 und 16 ist $27 \cdot 16 = 432$, dasjenige von 27 und 36 ist

$$36 \cdot \frac{27}{9} \quad \text{oder} \quad 27 \cdot \frac{36}{9} = 108.$$

Hilfssatz. Wenn zwei Zahlen a , b in einer Zahl m aufgehen, so geht auch ihr kleinstes Vielfache v in m auf.

Beweis. Ginge v nicht in m auf, so würde die Division von m durch v einen Quotienten q und einen Rest $r < v$ ergeben; es wäre also $m = qv + r$. Da nun a und b in m und ebenso in v aufgehen, so müßten sie auch in dem Rest r aufgehen, und das ist wegen $r < v$ unmöglich.

2. Aufgabe. Das kleinste Vielfache mehrerer Zahlen a , b , c , ... zu finden.

Man bestimme das kleinste Vielfache der beiden Zahlen a und b ; dasselbe sei m . Dann geht die dritte Zahl c entweder in m auf oder nicht. Wir nehmen erstens an, c gehe in m auf; dann ist, da auch a und b in m aufgehen, m ein Vielfaches von a , b , c , und es läßt sich beweisen, daß m das kleinste Vielfache dieser drei Zahlen ist. Wäre nämlich das kleinste Vielfache von a , b , c eine Zahl $m' < m$, so müßte, da a , b , c in

m' aufgehen, auch a und b und daher auch das kleinste Vielfache von a und b , d. i. m in m' aufgehen. Das ist aber unmöglich, da $m > m'$ vorausgesetzt wird. Daher giebt es kein Vielfaches der Zahlen a, b, c , das kleiner als m ist, oder m ist das kleinste Vielfache von a, b, c .

Zweitens nehmen wir an, c gehe in m nicht auf, und bestimmen das kleinste Vielfache der beiden Zahlen c und m . Dasselbe sei m_1 . Weil dann die Zahlen a und b in m aufgehen und m ein Divisor von m_1 ist, so gehen a und b ebenfalls in m_1 auf. Es geht aber auch c in m_1 auf. Somit ist m_1 ein Vielfaches der drei Zahlen a, b, c , und wir behaupten, daß m_1 das kleinste Vielfache von a, b, c sei. Gingen nämlich die drei Zahlen a, b, c in einer Zahl $m'_1 < m_1$ auf, so würden auch a und b in m'_1 aufgehen, und daher müßte das kleinste Vielfache von a und b , d. i. m ein Divisor von m'_1 sein. Es geht aber auch c in m'_1 auf. Folglich würden m und c , und somit auch das kleinste Vielfache von m und c , d. i. m_1 in m'_1 aufgehen. Das ist aber unmöglich, da $m'_1 < m_1$ ist. Daher gehen a, b, c in keiner Zahl auf, die kleiner als m_1 ist, oder m_1 ist das kleinste Vielfache der drei Zahlen a, b, c .

Durch Fortsetzung dieser Schlüsse wird das kleinste Vielfache beliebig vieler Zahlen gefunden.

Beispiel. Es soll das kleinste Vielfache der Zahlen 504, 240 und 864 gefunden werden. Da

$$504 : 240 = 21 : 10$$

ist, so erhält man als kleinstes Vielfache der beiden ersten Zahlen $504 \cdot 10 = 5040$. Weiter ist

$$5040 : 864 = 35 : 6,$$

folglich ist das kleinste Vielfache aller drei Zahlen

$$5040 \cdot 6 = 30240,$$

was mit dem oben erhaltenen Resultat übereinstimmt.

Aufgabe. Zwei Zahlen zu finden, deren kleinstes Vielfache v und größter gemeinschaftlicher Divisor d gegeben sind.

Lösung. Die Zahlen seien $x = d\xi$ und $y = d\eta$, wo also ξ und η prim zu einander sind. Dann ist $v = d\xi\eta$, folglich

$$\xi\eta = \frac{v}{d}.$$

Wenn man also $\frac{v}{d}$ auf alle möglichen Arten in je zwei Faktoren zerlegt, die prim zu einander sind, so wird der eine Faktor ξ , der andere η sein. Hat man ξ und η bestimmt, so ergibt die Multiplikation mit d die Zahlen x und y .

Beispiel. Für $v = 5040$ und $d = 30$ ist

$$\frac{v}{d} = 168 = 168.1 = 56.3 = 24.7 = 21.8,$$

somit

ξ	168	56	24	21
η	1	3	7	8
x	5040	1680	720	630
y	30	90	210	240.

§. 19.

Über die Anzahl der Zahlen, welche prim zu einer Zahl und nicht größer als dieselbe sind. — Summe dieser Zahlen (Euler, Commentationes arithmet. coll. I, p. 274 und II, p. 127).

Es soll bestimmt werden, wieviele Zahlen der Reihe 1, 2, 3, ..., m prim zu m sind. Die Anzahl dieser Zahlen pflegt man mit $\varphi(m)$ zu bezeichnen.

Zu 1 ist nur die Zahl 1 prim, und da zugleich 1 nicht größer als 1 ist¹⁾, so ergibt sich $\varphi(1) = 1$.

Zu 2 ist ebenfalls nur die Zahl 1 prim; also ist auch $\varphi(2) = 1$.

Prim zu 3 sind die beiden Zahlen 1 und 2; folglich ist $\varphi(3) = 2$.

So erhält man weiter

$\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, $\varphi(7) = 6$, $\varphi(8) = 4$, u. s. w.

Ehe wir zur Bestimmung von $\varphi(m)$ im allgemeinsten Falle übergehen, wollen wir den Wert dieser Funktion in einigen besonderen Fällen ermitteln.

¹⁾ Von diesem Falle abgesehen, ist jede der Zahlen 1, 2, 3, ..., m , wenn sie prim zu m ist, auch $< m$. Wir werden daher in der Folge statt „nicht größer als“ meist auch „kleiner als“ sagen können.

Am einfachsten ist es, wenn m eine Primzahl ist. Dann sind die Zahlen $1, 2, 3, \dots, (m - 1)$, die kleiner als m sind, sämtlich prim zu m ; folglich ist in diesem Falle

$$\varphi(m) = m - 1 = m \left(1 - \frac{1}{m}\right).$$

Weiter sei m eine Potenz einer Primzahl, $m = p^n$. Dann ist die Anzahl aller Zahlen, die kleiner als m sind, gleich $p^n - 1$. Unter diesen befinden sich aber Zahlen, die nicht prim zu m sind; es sind das die unter p^n liegenden Vielfachen von p , aber keine anderen Zahlen, also

$$p, 2p, 3p, \dots, p^n - p;$$

da die Anzahl dieser Vielfachen von p gleich $p^{n-1} - 1$ ist, so erhalten wir

$$\begin{aligned} \varphi(p^n) &= p^n - 1 - (p^{n-1} - 1) = p^n - p^{n-1} = p^{n-1}(p - 1) \\ &= p^n \left(1 - \frac{1}{p}\right). \end{aligned}$$

Es möge jetzt m das Produkt zweier verschiedenen Primzahlen p und q sein, also $m = pq$. Dann ist die Anzahl der Zahlen, die kleiner als m sind, $pq - 1$. Von diesen Zahlen sind sowohl die Vielfachen von p

$$p, 2p, 3p, \dots, (q - 1)p,$$

deren Anzahl $q - 1$ beträgt, als auch die Vielfachen von q

$$q, 2q, 3q, \dots, (p - 1)q,$$

deren Anzahl $p - 1$ beträgt, wegzulassen, und da die Vielfachen von q von denjenigen von p verschieden sind, so ist die Anzahl der wegzulassenden Zahlen $p + q - 2$. Wir erhalten somit

$$\begin{aligned} \varphi(pq) &= pq - 1 - (p + q - 2) = pq - p - q + 1 \\ &= (p - 1)(q - 1) = pq \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{q}\right). \end{aligned}$$

Wenn m das Produkt dreier verschiedenen Primzahlen ist, $m = pqr$, so sind von den $pqr - 1$ Zahlen, die $< m$ sind, die $qr - 1$ Vielfachen von p

$$p, 2p, 3p, \dots, (qr - 1)p,$$

die $pr - 1$ Vielfachen von q und die $pq - 1$ Vielfachen von r , also im ganzen $qr + pr + pq - 3$ Zahlen wegzulassen. Auf

diese Weise sind aber die $r - 1$ Vielfachen von pq

$$pq, 2pq, 3pq, \dots, (r - 1)pq,$$

weil sie Vielfache von p und zugleich von q sind, zweimal in Wegfall gekommen, ebenso die $q - 1$ Vielfachen von pr und die $p - 1$ Vielfachen von qr . Die Anzahl der auszuschließenden Größen verringert sich also um

$$r - 1 + q - 1 + p - 1 = p + q + r - 3,$$

und wir erhalten

$$\begin{aligned} \varphi(pqr) &= pqr - 1 - (pq + pr + qr - 3) + (p + q + r - 3) \\ &= pqr - (pq + pr + qr) + (p + q + r) - 1 \\ &= (p - 1)(q - 1)(r - 1) = pqr \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{q}\right) \left(1 - \frac{1}{r}\right). \end{aligned}$$

Auf diese Weise ergibt sich, wenn $p, q, r, \dots, s$ von einander verschiedene Primzahlen bezeichnen,

$$\varphi(pqr \dots s) = pqr \dots s \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{q}\right) \left(1 - \frac{1}{r}\right) \dots \left(1 - \frac{1}{s}\right).$$

Wir nehmen jetzt an, m sei das Produkt aus einer Potenz einer Primzahl p in eine Primzahl q , $m = p^n q$. Dann sind $p^n q - 1$ Zahlen kleiner als m . Von diesen sind zunächst die $p^n - 1$ Vielfachen von q wegzulassen; es bleiben dann $p^n q - 1 - p^n + 1 = p^n q - p^n$ Zahlen. Läßt man weiter die $p^{n-1} q - 1$ Zahlen weg, die durch p teilbar sind, so bleiben $p^n q - p^n - p^{n-1} q + 1$ Zahlen. Es ist nun aber die Anzahl aller durch pq teilbaren Zahlen hinzuzufügen; denn diese Vielfachen von pq , deren Anzahl $p^{n-1} - 1$ beträgt, sind schon als Vielfache von q in Wegfall gekommen, dürfen also nicht noch einmal, weil sie auch Vielfache von p sind, weggelassen werden. Wir erhalten somit

$$\begin{aligned} \varphi(p^n q) &= p^n q - p^n - p^{n-1} q + 1 + p^{n-1} - 1 \\ &= p^n(q - 1) - p^{n-1}(q - 1) = p^{n-1}(p - 1)(q - 1) \\ &= p^n q \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{q}\right). \end{aligned}$$

Ist weiter m das Produkt einer Potenz der Primzahl p in eine Potenz der Primzahl q , $m = p^\alpha q^\beta$, so ist die Anzahl der

Zahlen, die kleiner als m sind, gleich . . . $p^\alpha q^\beta - 1$,

Vielfachen von p gleich $p^{\alpha-1} q^\beta - 1$,

" " q " $p^\alpha q^{\beta-1} - 1$,

" " $p q$ " $p^{\alpha-1} q^{\beta-1} - 1$,

folglich

$$\begin{aligned}\varphi(p^\alpha q^\beta) &= (p^\alpha q^\beta - 1) - (p^{\alpha-1} q^\beta - 1) - (p^\alpha q^{\beta-1} - 1) \\ &\quad + (p^{\alpha-1} q^{\beta-1} - 1) \\ &= p^\alpha q^\beta - p^{\alpha-1} q^\beta - p^\alpha q^{\beta-1} + p^{\alpha-1} q^{\beta-1} \\ &= (p^\alpha - p^{\alpha-1})(q^\beta - q^{\beta-1}) = p^\alpha q^\beta \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{q}\right).\end{aligned}$$

Allgemein ergibt sich auf diese Weise die Formel

$$\varphi(p^\alpha q^\beta \dots r^\gamma) = p^\alpha q^\beta \dots r^\gamma \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{q}\right) \dots \left(1 - \frac{1}{r}\right);$$

darin bezeichnen $p, q, \dots, r$ von einander verschiedene Primzahlen, $\alpha, \beta, \dots, \gamma$ ganze positive Zahlen¹⁾.

Beispiele:

$$\varphi(9) = \varphi(3^2) = 3 \cdot 2 = 6,$$

$$\begin{aligned}\varphi(504) &= \varphi(2^3 \cdot 3^2 \cdot 7) = 504 \cdot \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{7}\right) \\ &= 504 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{6}{7} = 144\end{aligned}$$

oder

$$\varphi(504) = 2^2 \cdot 3 \cdot 2 \cdot 6 = 144.$$

Anmerkung. Die Bestimmung von $\varphi(m)$ ist ein besonderer Fall der von A. Thacker in Crelles Journal XL behandelten Aufgabe: Die Summe der n^{ten} Potenzen aller Zahlen zu finden, die prim zu m und nicht gröfser als m sind. Wenn nämlich $n = 0$ gesetzt wird, so wird jedes Glied gleich 1, die Summe selbst also gleich der Anzahl der in Rede stehenden Zahlen.

Aufgabe. Die Summe der Zahlen zu bestimmen, welche prim zu einer gegebenen Zahl und nicht gröfser als dieselbe sind.

Wenn a prim zu m ist, so ist auch $m - a$ prim zu m . Die in Rede stehenden Zahlen lassen sich also in Gruppen von je

¹⁾ Des leichteren Verständnisses wegen bin ich in der Herleitung des Ausdrucks für $\varphi(m)$ Euler gefolgt. Eine allgemeinere und infolge davon kürzere Darstellung findet der Leser in meinem 1887 im Verlag von B. G. Teubner in Leipzig erschienenen Werk: „Elemente der Zahlentheorie“.

zweien so zusammenstellen, daß die Summe der Zahlen jeder Gruppe m ist. Da nun $\varphi(m)$ solcher Zahlen, also $\frac{1}{2} \varphi(m)$ Gruppen da sind, so ergibt sich für die gesuchte Gesamtsumme

$$\frac{1}{2} m \cdot \varphi(m).$$

Beispiele. I. Es ist

$$\varphi(60) = \varphi(2^2 \cdot 3 \cdot 5) = 2 \cdot 2 \cdot 4 = 16,$$

folglich ist die Summe der 16 Zahlen, die prim zu 60 und nicht größer als 60 sind, $\frac{1}{2} \cdot 16 \cdot 60 = 480$.

II. Da $\varphi(2^\alpha) = 2^{\alpha-1}$ ist, so ist die Summe aller ungeraden Zahlen von 1 bis $2^\alpha - 1$ gleich

$$\frac{1}{2} \cdot 2^{\alpha-1} \cdot 2^\alpha = 2^{2\alpha-2} = (2^{\alpha-1})^2.$$

1. Lehrsatz. Wenn M und N zwei relative Primzahlen sind, so ist

$$\varphi(MN) = \varphi(M) \cdot \varphi(N).$$

Beweis. Die in M aufgehenden ungleichen Primzahlen seien $m, m', m'', \dots$, die in N aufgehenden $n, n', n'', \dots$; dann ist, wie wir oben gesehen haben,

$$\varphi(M) = M \left(1 - \frac{1}{m}\right) \left(1 - \frac{1}{m'}\right) \dots,$$

$$\varphi(N) = N \left(1 - \frac{1}{n}\right) \left(1 - \frac{1}{n'}\right) \dots$$

Ferner ist, da die Primzahlen $m, m', m'', \dots, n, n', n'', \dots$ sämtlich von einander verschieden sind,

$$\varphi(MN) = MN \left(1 - \frac{1}{m}\right) \left(1 - \frac{1}{m'}\right) \dots \left(1 - \frac{1}{n}\right) \left(1 - \frac{1}{n'}\right) \dots,$$

somit

$$\varphi(MN) = \varphi(M) \cdot \varphi(N).$$

Zusatz. Wenn jede der Zahlen $M, N, P, \dots$ prim zu jeder anderen ist, so ist

$$\varphi(MNP\dots) = \varphi(M) \cdot \varphi(N) \cdot \varphi(P) \dots$$

Beweis. Es ist M prim zu $NP\dots$, folglich ist nach dem vorhergehenden Satze

$$\varphi(MNP\dots) = \varphi M \cdot \varphi(NP\dots).$$

Ebenso ist

$$\varphi(NP\dots) = \varphi(N) \cdot \varphi(P\dots) = \varphi(N) \varphi(P)\dots,$$

somit

$$\varphi(MNP\dots) = \varphi(M) \cdot \varphi(N) \cdot \varphi(P)\dots$$

Beispiel:

$$\varphi(300) = \varphi(4) \varphi(3) \varphi(25) = 2 \cdot 2 \cdot 20 = 80.$$

2. Lehrsatz. Wenn $a, a', a'', \dots$ die sämtlichen Divisoren von A sind (die Einheit und die Zahl A selbst nicht ausgeschlossen), so ist

$$\varphi(a) + \varphi(a') + \varphi(a'') + \dots = A.$$

I. Beweis (Gauss, Disquisitiones 39). Man multipliziere alle Zahlen, die prim zu a und nicht größer als a sind, mit $\frac{A}{a}$, ebenso alle Zahlen, die prim zu a' und nicht größer als a' sind, mit $\frac{A}{a'}$, u. s. w., so erhält man $\varphi(a) + \varphi(a') + \dots$ Zahlen, die sämtlich nicht größer als A sein werden.

Diese Zahlen sind nun aber erstens ungleich. Dafs die Zahlen, welche aus demselben Divisor von A hervorgehen, ungleich sind, ist an sich klar. Wenn nun aus den verschiedenen Divisoren M, N und den mit diesen beziehungsweise teilerfremden Zahlen μ, ν gleiche Zahlen hervorgingen, d. h. wenn $\frac{A}{M} \mu = \frac{A}{N} \nu$ wäre, so würde $\mu N = \nu M$ folgen. Wir nehmen jetzt an, was gestattet ist, es sei $M > N$. Da die Zahl M prim zu μ ist und in μN aufgehen soll, so mufs sie in N aufgehen, und das ist wegen $M > N$ unmöglich. Somit sind die erhaltenen Zahlen in der That sämtlich ungleich.

Zweitens beweisen wir, dafs sich unter diesen Zahlen alle Zahlen $1, 2, 3, \dots, A$ vorfinden. Es sei t irgend eine der Zahlen, die nicht größer als A sind, und δ der grösste gemeinschaftliche Divisor von A und t . Dann ist $\frac{A}{\delta}$ ein Divisor von A , zu welchem

$\frac{t}{\delta}$ prim ist. Somit befindet sich t unter den Zahlen, die aus dem Divisor $\frac{A}{\delta}$ entstehen.

Wir erhalten auf die dargelegte Weise also alle Zahlen 1, 2, 3, ..., A , und da die Anzahl dieser Zahlen gleich A ist, so ergibt sich

$$\varphi(a) + \varphi(a') + \varphi(a'') + \dots = A.$$

II. Beweis (Emil Strauss, mündliche Mitteilung). Wir betrachten die Reihe der Brüche

$$\frac{1}{A}, \frac{2}{A}, \frac{3}{A}, \dots, \frac{A}{A}$$

und denken uns jeden derselben in den kleinsten Zahlen ausgedrückt. Unter den Nennern der so erhaltenen Brüche muß dann jeder Divisor a von A vorkommen und zwar in $\varphi(a)$ Brüchen, also $\varphi(a)$ mal.

Ist nämlich k irgend eine der $\varphi(a)$ Zahlen, die prim zu a und nicht größer als a sind, so wird sich der Bruch $\frac{k}{a}$ unter jenen Brüchen vorfinden; denn wenn wir $\frac{k}{a}$ mit der ganzen Zahl $\mu = \frac{A}{a}$ erweitern, so ergibt sich $\frac{\mu k}{\mu a} = \frac{\mu k}{A}$, und da $k < a$, also $\mu k < \mu a$, d. i. $\mu k < A$ ist, so befindet sich der Bruch $\frac{\mu k}{A}$ unter den gegebenen und sein reduzierter Wert $\frac{k}{a}$ unter den reduzierten Brüchen. Es sind daher $\varphi(a)$ Brüche mit dem Nenner a , $\varphi(a')$ Brüche mit dem Nenner a' , $\varphi(a'')$ Brüche mit dem Nenner a'' , u. s. w. vorhanden, und da die Gesamtzahl aller Brüche A ist, so muß

$$\varphi(a) + \varphi(a') + \varphi(a'') + \dots = A$$

sein.

Anmerkung. Beide vorhergehenden Beweise sind nur in der Form von einander verschieden.

Beispiel. 40 hat die acht Divisoren

$$1, 2, 4, 5, 8, 10, 20, 40.$$

Es ist

$$\varphi(1) = 1, \quad \varphi(2) = 1, \quad \varphi(4) = 2, \quad \varphi(5) = 4, \quad \varphi(8) = 4, \\ \varphi(10) = 4, \quad \varphi(20) = 8, \quad \varphi(40) = 16$$

und

$$1 + 1 + 2 + 4 + 4 + 4 + 8 + 16 = 40.$$

Aufgaben. Beweise folgende Sätze:

1. Es giebt $\varphi(n)$ echte irreducibele Brüche mit dem Nenner n .
2. Es giebt $\varphi(2) + \varphi(3) + \varphi(4) + \dots + \varphi(m)$ echte irreducibele Brüche, deren Nenner die gegebene Zahl m nicht überschreitet.
3. Sobald $m > 2$ ist, ist $\varphi(m)$ immer eine gerade Zahl.
4. Wenn m eine ungerade Zahl bezeichnet, so ist $\varphi(2m) = \varphi(m)$.
5. Die Summe aller echten irreducibelen Brüche mit dem Nenner $n > 2$ ist eine ganze Zahl und zwar gleich $\frac{1}{2} \varphi(n)$.

6. Für welche Zahlen hat die Function φ den Wert 12?

Es ist $12 = 1.12 = 2.6$. Da $\varphi(m)$ für $m > 2$ eine gerade Zahl ist, so ist die Zerlegung $12 = 3.4$ unzulässig. Der Zerlegung 1.12 entsprechen, da $\varphi(1) = \varphi(2) = 1$ und $\varphi(13) = 12$ ist, die Zahlen $1.13 = 13$ und $2.13 = 26$.

Der Zerlegung 2.6 entsprechen, da $\varphi(3) = \varphi(4) = \varphi(6) = 2$ und $\varphi(7) = \varphi(9) = \varphi(14) = \varphi(18) = 6$ ist, die Zahlen $3.7 = 21$, $3.14 = 42$, $4.7 = 28$, $4.9 = 36$. Die übrigen Verbindungen sind unzulässig, da man nur zwei Faktoren zusammen nehmen kann, welche prim zu einander sind. Es ergeben sich also die sechs Zahlen

$$13, \quad 21, \quad 26, \quad 28, \quad 36, \quad 42.$$

7. Für welche Zahlen n ist $\varphi(n) = 24$?

$$35, \quad 39, \quad 45, \quad 52, \quad 56, \quad 70, \quad 72, \quad 78, \quad 84, \quad 90.$$

Anmerkung. Die vorhergehende Aufgabe hat für viele Werte von $\varphi(n)$ überhaupt keine Lösung. Unter 100 sind dies die Werte

$$\varphi(n) = 14, \quad 26, \quad 34, \quad 38, \quad 50, \quad 62, \quad 68, \quad 74, \quad 76, \quad 86, \quad 90, \quad 94 \text{ und } 98.$$

§. 20.

Höchste Potenz einer Primzahl, welche in dem Produkt aller Zahlen von 1 bis n aufgeht. (Legendre, Théorie des Nombres, Introduction XVI etc.)

Es soll bestimmt werden, wieviel mal eine gegebene Primzahl p Faktor in der Reihe der natürlichen Zahlen von 1 bis n ist oder, was auf dasselbe hinausläuft, welches die höchste Potenz von p ist, die in dem Produkt $1.2.3\dots n$ aufgeht.

Wir bezeichnen die grösste in dem Bruche $\frac{n}{a}$ enthaltene ganze Zahl mit $E\left(\frac{n}{a}\right)$ und die gesuchte Zahl oder den Exponenten von p mit x . Dann ergibt sich

$$x = E\left(\frac{n}{p}\right) + E\left(\frac{n}{p^2}\right) + E\left(\frac{n}{p^3}\right) + \dots,$$

und zwar ist diese Reihe so lange fortzusetzen, als der Zähler gröfser wie der Nenner ist.

Offenbar stellt nämlich $E\left(\frac{n}{p}\right)$ die Anzahl der Glieder der Reihe 1, 2, 3, ..., n dar, die durch p teilbar sind, ebenso $E\left(\frac{n}{p^2}\right)$ die Anzahl der durch p^2 teilbaren Glieder derselben Reihe, u. s. w. Wenn nun das Produkt $1.2.3\dots n$ keine durch p^2 teilbaren Glieder enthielte, so würde die Anzahl der in demselben aufgehenden Faktoren p einfach $E\left(\frac{n}{p}\right)$ sein. Wenn dann noch durch p^2 teilbare Glieder vorhanden sind, so fügt jedes der letzteren einen neuen Faktor p den schon in $E\left(\frac{n}{p}\right)$ enthaltenen hinzu. Infolge davon wird die Anzahl der Faktoren p , welche von den durch p und den durch p^2 teilbaren Gliedern herrühren, gleich $E\left(\frac{n}{p}\right) + E\left(\frac{n}{p^2}\right)$. Ebenso fügt jedes durch p^3 teilbare Glied des Produktes einen weiteren Faktor p den schon gezählten hinzu, so dafs die Gesamtzahl der Faktoren p gleich

$$E\left(\frac{n}{p}\right) + E\left(\frac{n}{p^2}\right) + E\left(\frac{n}{p^3}\right)$$

wird. Das geht so fort, bis man zu einer Potenz p^i gelangt, die $> n$ ist. Dann ist die Reihe der E zu Ende; denn, wenn $\frac{n}{p^i} < 1$ ist, so ist $E\left(\frac{n}{p^i}\right) = 0$.

Suchen wir z. B. zu bestimmen, wie oft das Produkt der Zahlen von 1 bis 10000 den Faktor 7 enthält. Die zu diesem Zwecke auszuführende Rechnung gestaltet sich folgendermaßen: Es ist

$$E\left(\frac{10000}{7}\right) = 1428,$$

$$E\left(\frac{10000}{7^2}\right) = E\left(\frac{1428}{7}\right) = 204,$$

$$E\left(\frac{10000}{7^3}\right) = E\left(\frac{204}{7}\right) = 29,$$

$$E\left(\frac{10000}{7^4}\right) = E\left(\frac{29}{7}\right) = 4,$$

$$E\left(\frac{10000}{7^5}\right) = E\left(\frac{4}{7}\right) = 0.$$

Die Summe aller dieser Zahlen ist 1665. Das Produkt der Zahlen von 1 bis 10000 ist also durch 7^{1665} teilbar.

Wenn die vorgelegte Zahl n eine Potenz von 7 gewesen wäre, so würde man

$$x = \frac{n-1}{6}$$

erhalten haben. Ist allgemein $n = p^m$, so erhält man für die Anzahl x der in dem Produkt $1.2.3\dots n$ enthaltenen Faktoren p

$$x = \frac{n-1}{p-1}.$$

Man kann nun immer

$$n = ap^m + bp^n + cp^0 + \dots$$

voraussetzen, wo die Koeffizienten $a, b, c, \dots$ kleiner als p sind. Dann ergibt sich leicht

$$x = \frac{n - a - b - c - \dots}{p - 1}.$$

In dem besonderen Falle $n = 2^m, p = 2$ erhält man

$$x = n - 1,$$

und wenn man allgemein

$$n = 2^m + 2^n + 2^o + \dots$$

macht, so ergibt sich

$$x = n - k,$$

wo k die Anzahl der Glieder $2^m, 2^n, 2^o, \dots$ bezeichnet, aus denen der Wert von n besteht.

Will man z. B. wissen, wie oft der Faktor 2 in der Reihe der natürlichen Zahlen von 1 bis 1000 enthalten ist, so zerlegt man 1000 in Potenzen von 2:

$$1000 = 2^9 + 2^8 + 2^7 + 2^6 + 2^5 + 2^3.$$

Da die Anzahl der Glieder, in die 1000 zerfällt, 6 ist, so ist die gesuchte Zahl $1000 - 6 = 994$.

Zu demselben Resultate hätte man ebenso leicht mittels der allgemeinen Formel gelangen können. Es ist nämlich

$$E\left(\frac{1000}{2}\right) = 500, \quad E\left(\frac{500}{2}\right) = 250, \quad E\left(\frac{250}{2}\right) = 125,$$

$$E\left(\frac{125}{2}\right) = 62, \quad E\left(\frac{62}{2}\right) = 31, \quad E\left(\frac{31}{2}\right) = 15,$$

$$E\left(\frac{15}{2}\right) = 7, \quad E\left(\frac{7}{2}\right) = 3, \quad E\left(\frac{3}{2}\right) = 1,$$

und die Summe aller dieser Zahlen beträgt 994.

Ebenso folgt aus der Zerlegung

$$1000 = 5^4 + 3 \cdot 5^3,$$

da

$$\frac{1000 - 1 - 3}{5 - 1} = 249$$

ist, daß das Produkt $1 \cdot 2 \cdot 3 \dots 1000$ den Faktor 5^{249} enthält; die allgemeine Formel würde

$$E\left(\frac{1000}{5}\right) = 200, \quad E\left(\frac{200}{5}\right) = 40, \quad E\left(\frac{40}{5}\right) = 8, \quad E\left(\frac{8}{5}\right) = 1,$$

also, da

$$200 + 40 + 8 + 1 = 249$$

ist, dasselbe Resultat liefern.

Lehrsatz. Wenn $n, p, q, r, \dots$ ganze Zahlen sind, welche der Bedingung

$$n = p + q + r + \dots$$

genügen, so ist

$$A = \frac{1.2.3\dots n}{1.2.3\dots p.1.2.3\dots q.1.2.3\dots r\dots} \quad ^1)$$

eine ganze Zahl.

Beweis. Es sei a eine beliebige der Primzahlen, die in dem Nenner und somit auch in dem Zähler von A aufgehen. Der Exponent der höchsten im Zähler enthaltenen Potenz von a wird dann

$$E\left(\frac{n}{a}\right) + E\left(\frac{n}{a^2}\right) + \dots = E\left(\frac{p+q+r+\dots}{a}\right) \\ + E\left(\frac{p+q+r+\dots}{a^2}\right) + \dots$$

sein, der Exponent der höchsten Potenz von a , die der Nenner enthält:

$$E\left(\frac{p}{a}\right) + E\left(\frac{p}{a^2}\right) + \dots + E\left(\frac{q}{a}\right) + E\left(\frac{q}{a^2}\right) + \dots + E\left(\frac{r}{a}\right) + \dots$$

Nun ist aber offenbar

$$E\left(\frac{p+q+r+\dots}{a}\right) \geq E\left(\frac{p}{a}\right) + E\left(\frac{q}{a}\right) + E\left(\frac{r}{a}\right) + \dots$$

$$E\left(\frac{p+q+r+\dots}{a^2}\right) \geq E\left(\frac{p}{a^2}\right) + E\left(\frac{q}{a^2}\right) + E\left(\frac{r}{a^2}\right) + \dots$$

folglich geht jede im Nenner enthaltene Primzahl a mindestens ebenso oft in dem Zähler auf, d. h. der Zähler ist durch den Nenner teilbar oder A ist eine ganze Zahl.

Zusatz. Das Produkt von m beliebigen aufeinander folgenden Zahlen ist durch das Produkt der m ersten Zahlen teilbar.

Beweis. Es ist

$$A = \frac{(a+1)(a+2)\dots(a+m)}{1.2.3\dots m} = \frac{1.2.3\dots a(a+1)\dots(a+m)}{1.2.3\dots a.1.2.3\dots m},$$

also A nach dem vorhergehenden Satze eine ganze Zahl.

¹⁾ Es ist dies der Koeffizient von $x^p y^q z^r \dots$ in der Entwicklung von $(x+y+z+\dots)^n$.

§. 21.

Anzahl der Zahlen eines gegebenen Gebiets, welche durch gegebene Primzahlen nicht teilbar sind. (Legendre, Théorie des nombres II, p. 86 ff.)

1. Aufgabe. Es soll bestimmt werden, wieviele Zahlen der Reihe

$$(1) \quad 1, 2, 3, \dots, n$$

durch die Primzahlen $p, q, r, \dots, s$ nicht teilbar sind.

Wenn zunächst n ein Vielfaches von p , etwa $n = kp$ ist, so enthält die Reihe (1) die k durch p teilbaren Zahlen

$$p, 2p, 3p, \dots, kp,$$

also

$$n - k = n - \frac{n}{p} = n \left(1 - \frac{1}{p}\right)$$

Zahlen, welche durch p nicht teilbar sind.

Wenn n kein Vielfaches von p ist und wieder $E\left(\frac{n}{p}\right)$ die größte ganze Zahl bezeichnet, die in dem Bruch $\frac{n}{p}$ enthalten ist, so ergibt sich, daß die Reihe (1)

$$n - E\left(\frac{n}{p}\right)$$

Zahlen enthält, die durch p nicht teilbar sind.

Um weiter zu bestimmen, wieviele von den Zahlen (1) weder durch p , noch durch q teilbar sind, scheiden wir zunächst die $E\left(\frac{n}{p}\right)$ durch p teilbaren, dann die $E\left(\frac{n}{q}\right)$ durch q teilbaren aus; dadurch würden wir

$$n - E\left(\frac{n}{p}\right) - E\left(\frac{n}{q}\right)$$

erhalten; wir haben aber jede der $E\left(\frac{n}{pq}\right)$ durch das Produkt pq teilbaren Zahlen zweimal ausgeschieden. Die Reihe (1) enthält also

$$n - E\left(\frac{n}{p}\right) - E\left(\frac{n}{q}\right) + E\left(\frac{n}{pq}\right)$$

Zahlen, welche weder durch p , noch durch q teilbar sind. Wenn n durch p und durch q , also auch durch pq teilbar ist, so geht dieser Ausdruck über in

$$n\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right).$$

Ist r eine dritte Primzahl, so ergibt sich die Anzahl der weder durch p , noch durch q , noch durch r teilbaren Zahlen der Reihe (1) auf folgende Weise:

Wir lassen erst die durch p , dann die durch q , endlich die durch r teilbaren Zahlen weg; dann bleiben

$$n - E\left(\frac{n}{p}\right) - E\left(\frac{n}{q}\right) - E\left(\frac{n}{r}\right)$$

Zahlen zurück. Nun ist aber jede der beziehungsweise durch pq , qr , pr teilbaren Zahlen zweimal ausgeschieden; also muß zu obigem Ausdruck noch

$$E\left(\frac{n}{pq}\right) + E\left(\frac{n}{qr}\right) + E\left(\frac{n}{pr}\right)$$

addiert werden. Endlich ist jede der $E\left(\frac{n}{pqr}\right)$ Zahlen, die durch das Produkt pqr teilbar sind, dreimal fortgelassen (weil durch p , durch q und durch r teilbar) und ebenso oft wieder hinzugefügt worden (weil durch pq , durch qr , durch pr teilbar). Da nun diese Zahlen aus (1) fortgelassen werden sollen, so ergibt sich, daß die Reihe (1)

$$\begin{aligned} n - E\left(\frac{n}{p}\right) - E\left(\frac{n}{q}\right) - E\left(\frac{n}{r}\right) + E\left(\frac{n}{pq}\right) + E\left(\frac{n}{qr}\right) \\ + E\left(\frac{n}{pr}\right) - E\left(\frac{n}{pqr}\right) \end{aligned}$$

Zahlen enthält, welche weder durch p , noch durch q , noch durch r teilbar sind. Wenn n durch p , q , r teilbar ist, so geht dieser Ausdruck über in

$$n\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{r}\right).$$

Durch Fortsetzung dieser Schlüsse erhalten wir das Resultat:

Man erhält die Anzahl der Zahlen der Reihe 1, 2, 3, ..., n , welche durch keine der Primzahlen p , q , r , ..., s teilbar sind, indem man das Produkt

$$n \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{q}\right) \left(1 - \frac{1}{r}\right) \dots \left(1 - \frac{1}{s}\right)$$

auflöst und jedes Glied unter Beibehaltung seines Vorzeichens durch die größte in ihm enthaltene ganze Zahl ersetzt.

Beispiel. Unter den Zahlen 1, 2, 3, ..., 50 befinden sich

$$50 \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{7}\right) \left(1 - \frac{1}{11}\right) = 50 \left[1 - \left(\frac{1}{3} + \frac{1}{7} + \frac{1}{11}\right) + \left(\frac{1}{21} + \frac{1}{33} + \frac{1}{77}\right) - \frac{1}{231}\right] = 50 - (16 + 7 + 4) + (2 + 1) = 26$$

Zahlen, welche weder durch 3, noch durch 7, noch durch 11 teilbar sind.

2. Aufgabe. Wir wollen bestimmen, wieviele Zahlen der Reihe 1, 2, 3, ..., n durch keine der i ersten Primzahlen

$$p_1 = 2, \quad p_2 = 3, \quad p_3 = 5, \dots, p_i$$

teilbar sind.

Die gesuchte Anzahl werde mit $\varphi(n, i)$ bezeichnet, so daß z. B.

$$\varphi(7, 1) = 4, \quad \varphi(8, 1) = 4, \quad \varphi(10, 2) = 3, \quad \text{u. s. w.}$$

ist.

Um aus der Reihe 1, 2, 3, ..., n alle Zahlen zu entfernen, welche durch eine der i ersten Primzahlen teilbar sind, scheiden wir zunächst alle diejenigen aus, welche eine der $(i-1)$ ersten Primzahlen als Faktor enthalten; es bleiben dann $\varphi(n, i-1)$ Zahlen zurück.

Von diesen haben wir noch die durch p_i teilbaren fortzuschaffen, also die Zahlen

$$p_i, \quad 2p_i, \quad 3p_i, \dots, \quad E\left(\frac{n}{p_i}\right)p_i.$$

Ein Teil dieser letzteren ist aber schon weggefallen, nämlich alle diejenigen, welche durch eine der $i-1$ ersten Primzahlen teilbar sind; es bleiben also nur die zu beseitigen, welche durch p_i , aber durch keine der vorhergehenden Primzahlen teilbar sind. Die Anzahl dieser letzteren stimmt überein mit der Anzahl der Zahlen der Reihe

$$1, \quad 2, \quad 3, \dots, \quad E\left(\frac{n}{p_i}\right),$$

welche durch keine der $i-1$ ersten Primzahlen teilbar sind, beträgt also

$$\varphi \left[E \left(\frac{n}{p_i} \right), i - 1 \right],$$

und somit erhalten wir für $\varphi(n, i)$ die Formel

$$\varphi(n, i) = \varphi(n, i - 1) - \varphi \left[E \left(\frac{n}{p_i} \right), i - 1 \right].$$

Beispiel. Es soll bestimmt werden, wieviel Zahlen der Reihe 1, 2, 3, ..., 2000 durch keine der fünf ersten Primzahlen 2, 3, 5, 7, 11 teilbar sind.

Es ist

$$2000 : 11 = 181, \dots,$$

also

$$\varphi(2000, 5) = \varphi(2000, 4) - \varphi(181, 4).$$

Weiter ist

$$2000 : 7 = 285, \dots, \quad 181 : 7 = 25, \dots,$$

also

$$\varphi(2000, 4) = \varphi(2000, 3) - \varphi(285, 3) = 534 - 76 = 458;$$

denn

$$\begin{aligned} \varphi(2000, 3) &= \varphi(2000, 2) - \varphi(400, 2) \\ &= \varphi(2000, 1) - \varphi(666, 1) - \varphi(400, 1) + \varphi(133, 1) \\ &= 1000 - 333 - 200 + 67 = 534. \end{aligned}$$

$$\begin{aligned} \varphi(285, 3) &= \varphi(285, 2) - \varphi(57, 2) \\ &= \varphi(285, 1) - \varphi(95, 1) - \varphi(57, 1) + \varphi(19, 1) \\ &= 143 - 48 - 29 + 10 = 76. \end{aligned}$$

Ebenso folgt

$$\varphi(181, 4) = \varphi(181, 3) - \varphi(25, 3) = 49 - 7 = 42;$$

denn

$$\begin{aligned} \varphi(181, 3) &= \varphi(181, 2) - \varphi(36, 2) \\ &= \varphi(181, 1) - \varphi(60, 1) - \varphi(36, 1) + \varphi(12, 1) \\ &= 91 - 30 - 18 + 6 = 49; \end{aligned}$$

$$\begin{aligned} \varphi(25, 3) &= \varphi(25, 2) - \varphi(5, 2) \\ &= \varphi(25, 1) - \varphi(8, 1) - \varphi(5, 1) + \varphi(1, 1) \\ &= 13 - 4 - 3 + 1 = 7. \end{aligned}$$

Es ergibt sich also $\varphi(2000, 5) = 458 - 42 = 416$, d. h. in dem Gebiet von 1 bis 2000 gibt es 416 Zahlen, welche weder durch 2, noch durch 3, noch durch 5, noch durch 7, noch durch 11 teilbar sind.

§. 22.

Über die Anzahl der Primzahlen zwischen 1 und einer beliebigen Zahl n .

Es bezeichne p_i die größte Primzahl, die $< \sqrt{n}$ ist. Dann sind zwischen 1 und n die Zahl 1 und die zwischen $\sqrt{n}$ und n liegenden Primzahlen durch keine der i ersten Primzahlen teilbar, und somit liegen zwischen $\sqrt{n}$ und n im ganzen $\varphi(n, i) - 1$ Primzahlen. Da nun noch i Primzahlen zwischen 1 und $\sqrt{n}$ liegen, so erhalten wir für die Anzahl der zwischen 1 und n liegenden Primzahlen den Ausdruck

$$\varphi(n, i) + i - 1,$$

dessen Berechnung für grofse Werte von n freilich nicht geringe Schwierigkeiten bietet.

Es sei, um ein Beispiel zu geben, $n = 1000$; dann ist $\sqrt{n} = 31, \dots$, und unter $\sqrt{n}$ liegen die 11 Primzahlen

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31.$$

Folglich liegen zwischen 1 und 1000

$$\varphi(1000, 11) + 11 - 1$$

Primzahlen. Nun ergibt sich

$$\begin{aligned} \varphi(1000, 11) &= \varphi(1000, 10) - \varphi(32, 10) = \varphi(1000, 10) - 2 \\ \varphi(1000, 10) &= \varphi(1000, 9) - \varphi(34, 9) = \varphi(1000, 9) - 3 \\ \varphi(1000, 9) &= \varphi(1000, 8) - \varphi(43, 8) = \varphi(1000, 8) - 7 \\ \varphi(1000, 8) &= \varphi(1000, 7) - \varphi(52, 7) = \varphi(1000, 7) - 9 \\ \varphi(1000, 7) &= \varphi(1000, 6) - \varphi(58, 6) = \varphi(1000, 6) - 11 \\ \varphi(1000, 6) &= \varphi(1000, 5) - \varphi(76, 5) = \varphi(1000, 5) - 17 \\ \varphi(1000, 5) &= \varphi(1000, 4) - \varphi(90, 4) = \varphi(1000, 4) - 21 \\ \varphi(1000, 4) &= \varphi(1000, 3) - \varphi(142, 3) = \varphi(1000, 3) - 38 \\ \varphi(1000, 3) &= \varphi(1000, 2) - \varphi(200, 2) = \varphi(1000, 2) - 67 \\ \varphi(1000, 2) &= \varphi(1000, 1) - \varphi(333, 1) = \varphi(1000, 1) - 167 \\ \varphi(1000, 1) &= 500. \end{aligned}$$

Es ist somit

$$\varphi(1000, 11) = 500 - 342 = 158$$

und

$$\varphi(1000, 11) + 11 - 1 = 168,$$

d. h. zwischen 1 und 1000 liegen 168 Primzahlen.

A n h a n g.

Meissels Zählung der Primzahlen eines gegebenen Gebiets.

Die Verteilung der Primzahlen in der Zahlenreihe ist eine ganz unregelmäßige. Das lehrt schon der Anblick der folgenden kleinen Tabelle:

Zwischen	Primzahlen	Zwischen	Primzahlen
1 und 100	25	800 und 900	15
100 " 200	21	900 " 1 000	14
200 " 300	16		
300 " 400	16	1 400 und 1 500	17
400 " 500	17		
500 " 600	14	79 700 und 79 800	3
600 " 700	16		
700 " 800	14	90 000 und 90 100	13

Gauss hat die Primzahlen für jedes Tausend bis zu 1 Million abgezählt (Bd. II, S. 436 ff.) und eine Näherungsformel für die Primzahlenmenge in einem gegebenen Gebiet aufgestellt. Auch andere Mathematiker haben diese Menge durch eine Formel oder auch durch eine transzendente Gleichung auszudrücken gesucht¹⁾.

Dagegen hat Meissel (Mathematische Annalen II und III) durch Verbesserung der vorstehenden Methode die Aufgabe gelöst, die wirkliche Zählung der Primzahlen in einem gegebenen Gebiet zurückzuführen auf die Zählung derselben in einem kleineren Gebiet. Das Verfahren, welches Meissel einschlägt, wollen wir jetzt darlegen.

Es bezeichne $\psi(n)$ die Anzahl der Primzahlen in dem Intervall von 1 bis n , und es werde vorausgesetzt, man habe die Primzahlenmenge für

¹⁾ Legendre, Théorie des Nombres, Quatrième Partie §. VIII; Tschekbyscheff in Liouvilles Journal XVII (dargestellt auch in Serret, Handbuch der höheren Algebra, deutsch von G. Wertheim, Bd. II, S. 173 ff.); Riemann, Monatsberichte der Berliner Akademie 1859 oder Werke, S. 145 ff.; Scheibner in der Zeitschrift für Mathematik und Physik 1860; Mertens in Crelles Journal 1878; J. Braun in der wissenschaftlichen Beilage zum Programm des Gymnasiums zu Trier, 1899.

jedes der Gebiete 1 bis $\sqrt[3]{n}$ und 1 bis $\sqrt{n}$, also $\psi \sqrt[3]{n}$ und $\psi \sqrt{n}$ bestimmt. Da das erste Gebiet kleiner als das zweite ist, so wird es im allgemeinen auch weniger Primzahlen enthalten. Wir setzen demgemäß

$$\psi \sqrt[3]{n} = m, \quad \psi \sqrt{n} = m + \mu,$$

wo $\mu \geq 0$ ist. Bezeichnet jetzt s eine Zahl, welche der Bedingung $\mu \geq s \geq 0$ genügt, so ist nach der Formel, zu der wir in der 2. Aufgabe des §. 21 gelangt sind:

$$(1) \quad \varphi(n, m+s) = \varphi(n, m+s-1) - \varphi \left[E \left(\frac{n}{p_{m+s}}, m+s-1 \right) \right].$$

Nun ist p_m der Voraussetzung nach die größte Primzahl des Intervalls von 1 bis $\sqrt[3]{n}$, also

$$\frac{\sqrt[3]{n}}{p_{m+1}} < 1,$$

und daraus ergibt sich leicht

$$\frac{n}{p_{m+1}} < \sqrt[3]{n^2}, \quad \sqrt{\frac{n}{p_{m+1}}} < \sqrt[3]{n};$$

es ist also auch

$$\psi \sqrt{\frac{n}{p_{m+1}}} \leq \psi \sqrt[3]{n},$$

d. h.

$$m \geq \psi \sqrt{\frac{n}{p_{m+1}}}.$$

Für den Wert $s = 1$ besteht demnach die Ungleichung

$$m + s - 1 \geq \psi \sqrt{\frac{n}{p_{m+s}}},$$

und da bei zunehmendem s die linke Seite derselben offenbar größer, die rechte aber kleiner wird, so gilt diese Ungleichung für jedes $s \geq 1$.

Ferner enthält das Intervall von 1 bis $\sqrt{n}$ nach unserer Voraussetzung $m + \mu$ Primzahlen, von denen $p_{m+\mu}$ die größte ist. Es ist also

$$p_{m+\mu} \leq \sqrt{n}, \quad \frac{1}{p_{m+\mu}} \geq \frac{1}{\sqrt{n}}, \quad \frac{n}{p_{m+\mu}} \geq \sqrt{n}$$

und somit

$$\psi \left(\frac{n}{p_{m+\mu}} \right) \geq \psi \sqrt{n},$$

d. h.

$$\psi \left(\frac{n}{p_{m+\mu}} \right) \geq m + \mu > m + \mu - 1.$$

Für $s = \mu$ besteht demnach die Ungleichung

$$\psi \left(\frac{n}{p_{m+s}} \right) > m + s - 1,$$

und da bei abnehmendem s die linke Seite offenbar größer, die rechte kleiner wird, so gilt diese Ungleichung für jedes $s \leq \mu$.

Auf Grund unserer Voraussetzungen bestehen also für die Gültigkeit der Formel (1) die Grenzbedingungen

$$(2) \quad \psi\left(\frac{n}{p_m + s}\right) > m + s - 1 \geq \psi \sqrt{\frac{n}{p_m + s}},$$

und darin ist

$$\mu \geq s \geq 0.$$

Ehe wir aus der Formel (1) weitere Schlüsse ziehen, wollen wir das zweite Glied ihrer rechten Seite etwas umformen.

Nach der Definition drückt $\varphi(n, a)$ aus, wieviele Zahlen des Gebiets von 1 bis n durch keine der a ersten Primzahlen 2, 3, 5, ..., p_a teilbar sind. Es sind dies außer der Einheit die Primzahlen

$$p_{a+1}, p_{a+2}, \dots, p_{\psi(n)}$$

und die Produktverbindungen der letzteren. Wird aber die Bedingung

$$(3) \quad \psi(n) \geq a \geq \psi \sqrt{n}$$

gestellt, so ist $p_{a+1} > \sqrt{n}$, und folglich enthält das Intervall von 1 bis n keine Produktverbindung jener $\psi(n) - a$ Primzahlen; unter der Bedingung

(3) ist also

$$(4) \quad \varphi(n, a) = 1 + \psi(n) - a,$$

ein Resultat, zu dem wir schon im vorigen Paragraphen gelangt sind.

Die Formel (4) darf auf den Fall

$$n = E\left(\frac{n}{p_m + s}\right), \quad a = m + s - 1$$

angewendet werden; denn für diesen Fall fällt (2) mit der Bedingung (3) zusammen. Es ergibt sich

$$\varphi\left[E\left(\frac{n}{p_m + s}\right), m + s - 1\right] = 1 + \psi\left[E\left(\frac{n}{p_m + s}\right)\right] - (m + s - 1),$$

und dann geht (1), da

$$\psi\left(\frac{n}{p_m + s}\right)$$

statt

$$\psi\left[E\left(\frac{n}{p_m + s}\right)\right]$$

geschrieben werden kann, über in

$$\varphi(n, m + s) = \varphi(n, m + s - 1) - 2 + (m + s) - \psi\left(\frac{n}{p_m + s}\right).$$

Erteilt man hierin s der Reihe nach die Werte

$$\mu, \mu - 1, \mu - 2, \dots, 2, 1,$$

so erhält man die μ Gleichungen

$$\begin{aligned}
\varphi(n, m+\mu) &= \varphi(n, m+\mu-1) - 2 + (m+\mu) - \psi\left(\frac{n}{p_{m+\mu}}\right), \\
\varphi(n, m+\mu-1) &= \varphi(n, m+\mu-2) - 2 + (m+\mu) - 1 - \psi\left(\frac{n}{p_{m+\mu-1}}\right), \\
&\dots\dots\dots \\
\varphi(n, m+2) &= \varphi(n, m+1) - 2 + (m+\mu) - (\mu-2) - \psi\left(\frac{n}{p_{m+2}}\right), \\
\varphi(n, m+1) &= \varphi(n, m) - 2 + (m+\mu) - (\mu-1) - \psi\left(\frac{n}{p_{m+1}}\right),
\end{aligned}$$

durch deren Addition sich

$$\begin{aligned}
\varphi(n, m+\mu) &= \varphi(n, m) - 2\mu + \mu(m+\mu) - \frac{\mu(\mu-1)}{2} \\
&\quad - \left[\psi\left(\frac{n}{p_{m+1}}\right) + \psi\left(\frac{n}{p_{m+2}}\right) + \dots + \psi\left(\frac{n}{p_{m+\mu}}\right) \right]
\end{aligned}$$

ergibt. Nun ist $m + \mu = \psi \bar{V} n$ und

$$2\mu + \frac{\mu(\mu-1)}{2} = \frac{\mu(\mu+3)}{2},$$

also geht die letzte Formel, wenn zur Abkürzung noch

$$\psi\left(\frac{n}{p_{m+1}}\right) + \psi\left(\frac{n}{p_{m+2}}\right) + \dots + \psi\left(\frac{n}{p_{m+\mu}}\right) = \sum_{s=1}^{\mu} \psi\left(\frac{n}{p_{m+s}}\right)$$

gesetzt wird, über in

$$(5) \quad \varphi(n, \psi \bar{V} n) = \varphi(n, m) + \mu \psi \bar{V} n - \frac{\mu(\mu+3)}{2} - \sum_{s=1}^{\mu} \psi\left(\frac{n}{p_{m+s}}\right).$$

Nach der Formel (4) ist aber

$$\varphi(n, \psi \bar{V} n) = 1 + \psi(n) - \psi \bar{V} n,$$

und durch Einsetzung dieses Wertes in (5) erhält man nach leichten Umformungen

$$(6) \quad \psi(n) = \varphi(n, m) + (\mu+1)m + \frac{\mu(\mu-1)}{2} - 1 - \sum_{s=1}^{\mu} \psi\left(\frac{n}{p_{m+s}}\right).$$

Diese Formel dient zur Berechnung der Anzahl der Primzahlen zwischen 1 und n . Mittels derselben hat Meissel gefunden, daß innerhalb der ersten Hundert Millionen natürlicher Zahlen

5 761 460

Primzahlen vorkommen.

Beispiel. Für $n = 2000$ erhält man

$$\bar{V}^3 n = 12, \quad \bar{V} n = 44;$$

es ist also

$$m = 5, \quad \mu + m = 14, \quad \mu = 9,$$

und die Formel (6) liefert

$$\psi(2000) = \varphi(2000, 5) + 10 \cdot 5 + \frac{9 \cdot 8}{2} - 1 - \sum_{s=1}^{s=9} \psi\left(\frac{2000}{p_5+s}\right).$$

Nun ist

$$p_6 = 13, \quad \frac{2000}{13} = 153, \quad \psi(153) = 36$$

$$p_7 = 17, \quad \frac{2000}{17} = 117, \quad \psi(117) = 30$$

$$p_8 = 19, \quad \frac{2000}{19} = 105, \quad \psi(105) = 27$$

$$p_9 = 23, \quad \frac{2000}{23} = 86, \quad \psi(86) = 23$$

$$p_{10} = 29, \quad \frac{2000}{29} = 68, \quad \psi(68) = 19$$

$$p_{11} = 31, \quad \frac{2000}{31} = 64, \quad \psi(64) = 18$$

$$p_{12} = 37, \quad \frac{2000}{37} = 54, \quad \psi(54) = 16$$

$$p_{13} = 41, \quad \frac{2000}{41} = 48, \quad \psi(48) = 15$$

$$p_{14} = 43, \quad \frac{2000}{43} = 46, \quad \psi(46) = 14,$$

also

$$\sum_{s=1}^{s=9} \psi\left(\frac{2000}{p_5+s}\right) = 198,$$

und da nach der 2. Aufgabe des §. 21 $\varphi(2000, 5) = 416$ ist, so erhalten wir

$$\psi(2000) = 416 + 50 + 36 - 1 - 198 = 303,$$

d. h. das Gebiet von 1 bis 2000 enthält 303 Primzahlen.

Zweites Kapitel.

Kongruente Zahlen.

§. 23.

Definition kongruenter Zahlen.

Wenn die Differenz zweier Zahlen a, b durch eine dritte Zahl m ohne Rest teilbar, wenn also $\frac{a - b}{m}$ eine ganze Zahl ist, so nennt man a und b in Beziehung auf m kongruent. Die Zahl m heisst dann der Modul, und man schreibt nach Gauss' Vorgange

$$a \equiv b \pmod{m}.$$

So ist z. B.

$$40 \equiv 13 \pmod{9}, \quad 19 \equiv -1 \pmod{10},$$

da $40 - 13 = 27$ durch 9, $19 + 1 = 20$ durch 10 ohne Rest teilbar ist.

Anmerkung. Leonardo Pisano (Scritti ed. Boncompagni II, p. 265) und die von ihm abhängigen Mathematiker des Mittelalters, z. B. Paciolo (Summa, 1494 fol. 46 verso) und Ghaligai (Pratica d'Arithmetica, 1552 fol. 60 verso) gebrauchen die Ausdrücke numeri congrui und n. congruentes in einem anderen Sinne, und zwar bei der Lösung der Aufgabe: Eine Quadratzahl x^2 und eine Zahl y von der Beschaffenheit zu finden, daß sowohl $x^2 - y$, als auch $x^2 + y$ eine Quadratzahl sei, man also drei Quadratzahlen $x^2 - y, x^2, x^2 + y$ gleicher Differenz y erhalte. Leonardo Pisano nennt x^2 das congruens, y das congruum. Paciolo und Ghaligai haben die umgekehrte

Benennung angewandt. Als allgemeine Ausdrücke giebt Leonardo Pisano, wenn unter a und b beliebige ganze Zahlen verstanden werden:

$$x^2 = (a^2 + b^2)^2, \quad y = 4ab(a + b)(a - b).$$

In der That ist

$$\begin{aligned} (a^2 + b^2)^2 + 4ab(a + b)(a - b) &= (a^2 + 2ab - b^2)^2 \\ (a^2 + b^2)^2 - 4ab(a + b)(a - b) &= (a^2 - 2ab - b^2)^2. \end{aligned}$$

§. 24.

Reste einer Zahl.

Im bürgerlichen Rechnen nimmt man den Rest einer Division stets kleiner als den Divisor an. Wenn also die Division von a durch m den Quotienten q und den Rest r ergiebt, so daß $a = mq + r$ ist, so wird r als eine der Zahlen

$$0, 1, 2, \dots, (m - 1)$$

vorausgesetzt. Es leuchtet ein, daß man als Quotienten auch eine Zahl nehmen kann, die größer oder kleiner als q ist; der Rest wird dann im ersteren Falle negativ, im zweiten größer als m sein. Wenn nämlich $a = mq + r$ ist und unter s eine beliebige ganze positive Zahl verstanden wird, so ist auch

$$a = m(q + s) - (ms - r)$$

und ebenso

$$a = m(q - s) + (ms + r).$$

Wird im besonderen $s = 1$ angenommen, also der Quotient um 1 vergrößert, so hat man gleichzeitig

$$a = mq + r \quad \text{und} \quad a = m(q + 1) - (m - r),$$

und da, wenn $r > \frac{m}{2}$ ist, $m - r < \frac{m}{2}$ sein wird, so kann man den Quotienten immer so wählen, daß der Rest — abgesehen vom Vorzeichen — nicht größer als der halbe Divisor sei. Mit anderen Worten: Jede Zahl a besitzt in Beziehung auf den Divisor m einen positiven oder negativen Rest, dessen absoluter Betrag nicht größer als $\frac{1}{2}m$ ist. Diesen Rest nennt man den

absolut kleinsten Rest zum Unterschiede von dem kleinsten positiven Reste, der eine der Zahlen $0, 1, 2, 3, \dots, (m-1)$ ist.

Dividiert man z. B. 44 durch 9, so ergibt sich als kleinster positiver Rest 8, als absolut kleinster Rest -1 .

Aus der Annahme $a = mq + r$ folgt, daß $\frac{a-r}{m}$ eine ganze Zahl q , also $a \equiv r \pmod{m}$ ist. Jede Zahl ist somit ihrem Reste in Beziehung auf den Divisor als Modul kongruent.

Hat man umgekehrt $a \equiv r \pmod{m}$, so ist $\frac{a-r}{m}$ eine ganze Zahl, und wenn diese q genannt wird, so ergibt sich $a = mq + r$. Da nun a und r auch vertauschbar sind, so erhalten wir den Satz: Man kann jede von zwei für einen Modul kongruenten Zahlen als den Rest der anderen für diesen Modul als Divisor ansehen. Wegen dieser Beziehung bedient man sich des Ausdrucks „Rest“, ohne an eine Division zu denken. Wenn man $a \equiv b \pmod{m}$ hat, so ist einfach a der Rest von b und b der Rest von a für den Modul m .

§. 25.

Das vollständige Restsystem in Beziehung auf einen Modul.

Da jede beliebige ganze Zahl bei der Division durch m eine der m Zahlen

$$0, 1, 2, \dots, (m-1)$$

als Rest liefert, so können wir sämtliche Zahlen in m Klassen teilen. In die erste Klasse werden wir alle diejenigen stellen welche den Rest 0 geben, in die zweite diejenigen mit dem Reste 1, in die dritte diejenigen mit dem Reste 2, u. s. w. Es werden also zwei Zahlen in dieselbe Klasse oder in verschiedene Klassen kommen, je nachdem sie bei der Division durch m denselben Rest oder verschiedene Reste geben.

Bilden wir nun ein System von m Zahlen, indem wir aus jeder Klasse eine Zahl, gleichviel welche nehmen, so hat dieses System die Eigenschaft, daß jede beliebige Zahl einer und nur einer der m Zahlen des Systems kongruent ist. Die gewählten m Zahlen bilden ein vollständiges System nicht kongruenter Zahlen oder ein vollständiges Restsystem für den Modul

m . Ein solches System sind z. B. die positiven Reste (im engeren Sinne des Wortes) $0, 1, 2, \dots, (m - 1)$, ebenso die Zahlen $1, 2, 3, \dots, m$, überhaupt jede m aufeinander folgenden Zahlen.

§. 26.

Kongruenzen.

Drückt man aus, daß zwei Größen für einen Modul kongruent sind, so erhält man eine Kongruenz. Eine solche kann wie eine Gleichung eine oder mehrere Unbekannte enthalten und vom ersten, oder zweiten u. s. w. Grade in Beziehung auf die Unbekannten sein. So ist

$$8x \equiv 7 \pmod{11}$$

eine Kongruenz ersten Grades mit einer Unbekannten,

$$3x + 5y \equiv 8 \pmod{13}$$

eine Kongruenz ersten Grades mit zwei Unbekannten,

$$x^2 + 4x \equiv 4 \pmod{7}$$

eine Kongruenz zweiten Grades mit einer Unbekannten,

$$13x + 5y^2 \equiv 7 \pmod{16}$$

eine Kongruenz mit zwei Unbekannten, welche in Beziehung auf x vom ersten, in Beziehung auf y vom zweiten Grade ist; u. s. w.

§. 27.

Sätze über die Verbindung von Kongruenzen.

I. Wenn zwei Zahlen a und b einer dritten Zahl c für einen Modul m kongruent sind, so sind sie für denselben Modul einander kongruent.

Beweis. Da $a \equiv c \pmod{m}$ und $b \equiv c \pmod{m}$ ist, also $\frac{a-c}{m}$ und $\frac{b-c}{m}$ ganze Zahlen sind, so ist auch

$$\frac{a-c}{m} - \frac{b-c}{m} = \frac{a-b}{m}$$

eine ganze Zahl, d. h. $a \equiv b \pmod{m}$.

II. Wenn man die linken und ebenso die rechten Seiten mehrerer auf einen Modul bezüglichen Kongruenzen addiert, so erhält man eine für denselben Modul richtige Kongruenz.

Beweis. Ist

$$a_1 \equiv b_1, \quad a_2 \equiv b_2, \dots, \quad a_n \equiv b_n \pmod{m},$$

also jede der n Größen

$$\frac{a_1 - b_1}{m}, \quad \frac{a_2 - b_2}{m}, \dots, \quad \frac{a_n - b_n}{m}$$

eine ganze Zahl, so muß auch die Summe

$$\frac{a_1 - b_1}{m} + \frac{a_2 - b_2}{m} + \dots + \frac{a_n - b_n}{m},$$

d. i.

$$\frac{(a_1 + a_2 + \dots + a_n) - (b_1 + b_2 + \dots + b_n)}{m}$$

eine ganze Zahl sein, oder es ist

$$a_1 + a_2 + \dots + a_n \equiv b_1 + b_2 + \dots + b_n \pmod{m}.$$

Beispiel. Aus $13 \equiv 1$, $19 \equiv 7$, $34 \equiv -2$ und $29 \equiv 5 \pmod{12}$ folgt $95 \equiv 11 \pmod{12}$.

Zusatz. Eine Kongruenz bleibt richtig, wenn man jede Seite derselben mit einer Zahl n multipliziert.

Beweis. Wird der vorhergehende Satz auf die n identischen Kongruenzen

$$a \equiv b, \quad a \equiv b, \dots, \quad a \equiv b \pmod{m}$$

angewandt, so ergibt sich

$$na \equiv nb \pmod{m}.$$

Oder: Wenn $a \equiv b \pmod{m}$, also $\frac{a - b}{m}$ eine ganze Zahl ist, so ist auch $\frac{na - nb}{m}$ eine ganze Zahl, d. h.

$$na \equiv nb \pmod{m}.$$

Beispiel. Aus $15 \equiv -7 \pmod{11}$ folgt durch Multiplikation mit 3

$$45 \equiv -21 \pmod{11}.$$

III. Die Differenz zweier auf einen Modul bezüglichen Kongruenzen ist eine für denselben Modul richtige Kongruenz.

Beweis. Wenn $a_1 \equiv b_1, a_2 \equiv b_2 \pmod{m}$ ist, also

$$\frac{a_1 - b_1}{m} \text{ und } \frac{a_2 - b_2}{m}$$

ganze Zahlen sind, so ist auch

$$\frac{a_1 - b_1}{m} - \frac{a_2 - b_2}{m} = \frac{(a_1 - a_2) - (b_1 - b_2)}{m}$$

eine ganze Zahl, d. h.

$$a_1 - a_2 \equiv b_1 - b_2 \pmod{m}.$$

Beispiel. Aus $50 \equiv 2, 23 \equiv 7 \pmod{16}$ folgt

$$27 \equiv -5 \pmod{16}.$$

IV. Wenn man die linken und ebenso die rechten Seiten mehrerer auf einen Modul bezüglichen Kongruenzen multipliziert, so bilden die Produkte eine für denselben Modul richtige Kongruenz.

Beweis. Die gegebenen Kongruenzen

$$a_1 \equiv b_1, a_2 \equiv b_2, \dots, a_n \equiv b_n \pmod{m}$$

können durch die Gleichungen

$$a_1 = b_1 + m g_1, a_2 = b_2 + m g_2, \dots, a_n = b_n + m g_n$$

ersetzt werden, wo $g_1, g_2, \dots, g_n$ ganze Zahlen bedeuten. Durch Multiplikation dieser Gleichungen erhält man

$$a_1 a_2 \dots a_n = b_1 b_2 \dots b_n + m G,$$

wo G eine ganze Zahl bezeichnet, auf deren GröÙe es uns hier nicht ankommt. Es ist mithin

$$\frac{a_1 a_2 \dots a_n - b_1 b_2 \dots b_n}{m} = G,$$

d. h.

$$a_1 a_2 \dots a_n \equiv b_1 b_2 \dots b_n \pmod{m}.$$

Beispiel. Aus $10 \equiv 3, 5 \equiv -2, 22 \equiv 1 \pmod{7}$ folgt $1100 \equiv -6 \pmod{7}$.

Zusatz. Eine Kongruenz bleibt richtig, wenn man beide Seiten auf dieselbe Potenz erhebt.

Beweis. Wird in der letzten Kongruenz

$$\begin{aligned} a_1 &= a_2 = \dots = a_n = a \\ b_1 &= b_2 = \dots = b_n = b \end{aligned}$$

vorausgesetzt, so geht dieselbe über in

$$a^n \equiv b^n \pmod{m}.$$

Beispiel. Aus $5 \equiv -2 \pmod{7}$ folgt durch Erhebung auf die zweite Potenz

$$25 \equiv +4 \pmod{7}.$$

V. Wenn beide Glieder a, b einer Kongruenz

$$a \equiv b \pmod{m}$$

einen größten gemeinschaftlichen Divisor d haben, der prim zum Modul m ist, so gilt die durch beiderseitige Division mit d erhaltene Kongruenz ebenfalls für den Modul m .

Dieselbe gilt aber nur für den Modul $\frac{m}{\delta}$, wenn m und d den größten gemeinschaftlichen Divisor δ haben.

Beweis. Es sei $a = \alpha d, b = \beta d$, wo α und β prim zu einander sind. Nun soll

$$\frac{a-b}{m} = \frac{\alpha d - \beta d}{m} = \frac{d(\alpha - \beta)}{m}$$

eine ganze Zahl sein. Wenn also d prim zu m ist, so muß (§. 17, Satz I) m in $\alpha - \beta$ aufgehen, d. h. $\alpha \equiv \beta \pmod{m}$ sein.

Wenn aber d und m den größten gemeinschaftlichen Divisor δ haben, wenn etwa $d = \delta d_1, m = \delta m_1$ ist, wo d_1 und m_1 relative Primzahlen sind, so wird

$$\frac{d(\alpha - \beta)}{m} = \frac{d_1(\alpha - \beta)}{m_1},$$

und es muß $m_1 = \frac{m}{\delta}$ in $\alpha - \beta$ aufgehen, d. h. $\alpha \equiv \beta \pmod{\frac{m}{\delta}}$ sein.

Beispiele. Aus $40 \equiv 12 \pmod{7}$ folgt, da 4 prim zu 7 ist, $10 \equiv 3 \pmod{7}$.

Aus $65 \equiv 25 \pmod{10}$ folgt $13 \equiv 5 \pmod{2}$, nicht $\pmod{10}$.

VI. Wenn $a \equiv b \pmod{m}$ und d irgend ein Divisor von m ist, so ist auch $a \equiv b \pmod{d}$.

Beweis. Es sei $m = \mu d$. Da nun

$$\frac{a - b}{m} = \frac{a - b}{\mu d}$$

eine ganze Zahl ist, so muß auch $\frac{a - b}{d}$ eine ganze Zahl sein, d. h. es ist $a \equiv b \pmod{d}$.

VII. Wenn

$$a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \dots, a \equiv b \pmod{m_n}$$

ist und m das kleinste Vielfache von $m_1, m_2, \dots, m_n$ bezeichnet, so ist auch $a \equiv b \pmod{m}$.

Beweis. Da jede der Zahlen $m_1, m_2, \dots, m_n$ in $a - b$ aufgeht, so muß $a - b$ auch durch m ohne Rest teilbar sein.

Zusatz. Wenn jede der Zahlen $m_1, m_2, \dots, m_n$ zu jeder andern derselben prim ist, so ist m das Produkt der Zahlen; es besteht dann also die Kongruenz

$$a \equiv b \pmod{m_1 m_2 \dots m_n}.$$

Beispiele. Aus $64 \equiv 4 \pmod{6}, \pmod{10}, \pmod{15}$ folgt, da 30 das kleinste Vielfache von 6, 10, 15 ist,

$$64 \equiv 4 \pmod{30}.$$

Aus $113 \equiv 8 \pmod{3}, \pmod{5}, \pmod{7}$ folgt, da $3 \cdot 5 \cdot 7 = 105$ ist, $113 \equiv 8 \pmod{105}$.

§. 28.

Rechnungsproben.

Die Sätze des vorhergehenden Paragraphen begründen ein von den Indern erfundenes, von den Arabern weiter ausgebildetes und bis zum Ende des 16. Jahrhunderts allgemein angewandtes Verfahren, das Resultat einer Rechnung auf seine Richtigkeit zu prüfen. Hat man nämlich eine Reihe von Zahlen durch Addition, Subtraktion oder Multiplikation (Potenzierung) vereinigt, so ersetzt man jede Zahl durch ihren kleinsten Rest für irgend einen Modul (am zweckmäßigsten 9 oder 11). Vereinigt man dann diese Reste in derselben Weise wie vorher die gegebenen Zahlen,

so muß die aus den Resten hervorgehende Zahl der aus den Zahlen selbst erhaltenen für den gewählten Modul kongruent sein. Ist dies der Fall, so stimmt die Probe, und die Rechnung ist möglicherweise richtig. Stimmt die Probe nicht, so ist jedenfalls ein Fehler begangen.

Beispiele. Um zu sehen, ob wirklich

$$(15 + 54)13 - 325 = 572$$

ist, ersetze man links jede Zahl durch ihren kleinsten Rest für den Modul 9. Man erhält

$$(6 + 0)4 - 1 = 23 \equiv 5 \pmod{9},$$

und da auch $572 \equiv 5 \pmod{9}$ ist, so stimmt die Probe.

Um zu sehen, ob

$$(15^2 - 21)326 = 66504$$

ist, ersetze man links jede Zahl durch ihren Rest für den Modul 11. Man erhält

$$(4^2 - 10)7 = 6 \cdot 7 = 42 \equiv 9 \pmod{11},$$

und ebenso ist $66504 \equiv 9 \pmod{11}$ ¹⁾.

§. 29.

Teilbarkeitsregeln.

Die Sätze des §. 27 liefern auch Regeln zur Entscheidung, ob eine Zahl durch eine andere teilbar sei oder nicht.

I. Es sei zunächst P eine dekadisch geschriebene Zahl:

$$P = a + 10b + 10^2c + \dots,$$

enthalte also a Einer, b Zehner, c Hunderte, u. s. w. Wenn dann für einen Modul m

$$10 \equiv r_1, \quad 10^2 \equiv r_2, \dots$$

ist, so ist

¹⁾ Die Neunerprobe ist schon angewandt von Muhammed ibn Mûsâ Alchwarizmi (Algoritmi de Numero Indorum. Trattati d'Aritmetica pubblicati da Boncompagni I, p. 12), dann von Alkarkhi (Kâfi fil Hisâb, deutsch von Hochheim I, S. 8), von Leonardo Pisano (Scritti I, S. 9, 14, 20, 23), von Maximus Planudes (Rechenbuch, deutsch von Wäschke, S. 7) u. a. Leonardo Pisano wendet auch die Probe durch 7 und 11 an (l. c. S. 39, 45).

$$P \equiv a + r_1 b + r_2 c + \dots \pmod{m},$$

und wenn die rechte Seite durch m teilbar ist, so ist auch P durch m teilbar.

Beispiele. 1) Sowohl für den Modul 2, als auch für den Modul 5 ist

$$10 \equiv 0, \quad 10^2 \equiv 0, \quad \dots,$$

mithin

$$P \equiv a \pmod{2 \text{ und mod. } 5},$$

und dies drückt aus, daß eine Zahl durch 2 oder 5 teilbar ist, wenn die Anzahl ihrer Einer durch 2 oder 5 teilbar ist.

2) Sowohl für den Modul 3, als auch für den Modul 9 ist

$$10 \equiv 1, \quad 10^2 \equiv 1, \quad \dots,$$

mithin

$$P \equiv a + b + c + \dots \pmod{3 \text{ und mod. } 9},$$

und diese Formel lehrt den bekannten Satz: Jede Zahl giebt bei der Division durch 3 oder 9 denselben Rest wie ihre Quersumme.

3) Für den Modul 11 ist

$$10 \equiv -1, \quad 10^2 \equiv (-1)^2 \equiv +1, \quad 10^3 \equiv -1, \quad \dots,$$

folglich erhalten wir

$$P \equiv a - b + c - d + \dots \pmod{11},$$

und diese Formel drückt die bekannte Teilbarkeitsregel für den Divisor 11 aus.

4) Für den Modul 7 ist

$$10 \equiv 3, \quad 10^2 \equiv 2, \quad 10^3 \equiv -1, \quad 10^4 \equiv -3, \quad 10^5 \equiv -2, \\ 10^6 \equiv 1, \quad 10^7 \equiv 3 \quad \dots,$$

folglich

$$P \equiv (a + 3b + 2c) - (d + 3e + 2f) + \dots \pmod{7}.$$

Nach dieser Formel ist z. B.

$$348 \equiv 8 + 12 + 6 \equiv 26 \equiv 5 \pmod{7},$$

$$27653 \equiv (3 + 15 + 12) - (7 + 6) \equiv 17 \equiv 3 \pmod{7},$$

$$429730681 \equiv (1 + 24 + 12) - (9 + 14) + (9 + 6 + 8) \\ \equiv 37 - 23 + 23 \equiv 37 \equiv 2 \pmod{7}.$$

II. Weiter werde

$$P = a + 10b$$

vorausgesetzt, wo a die Einer und b die Zahl bezeichnet, die aus P bei Fortlassung der Einer wird. Dann ist es für gewisse Divisoren möglich, die Koeffizienten 1 und 10 durch Reste zu ersetzen, die ein bequemes Kennzeichen der Teilbarkeit durch diese Divisoren geben.

Beispiele. 1) Da $1 \equiv -6$, $10 \equiv 3 \pmod{7}$ ist, so ist

$$P \equiv -6a + 3b \equiv 3(b - 2a) \pmod{7},$$

und da 3 prim zu 7 ist, so wird P durch 7 teilbar sein, wenn $b - 2a$ es ist.

Danach ist 3192 durch 7 teilbar, wenn 7 in $319 - 4 = 315$ aufgeht; das ist aber der Fall, da $31 - 10 = 21$ durch 7 teilbar ist.

Wird in dem obigen Ausdruck für P die Zahl 2 durch die kongruente Zahl $2 + 7k$ ersetzt, so erhalten wir allgemeiner

$$P \equiv 3[b - (2 + 7k)a] \pmod{7};$$

k kann jede ganze Zahl sein. Wenn wir etwa $k = 45$ annehmen, so daß

$$P \equiv 3[b - 317a] \pmod{7}$$

wird, so haben wir, um die Zahl 13734 zu prüfen, die Differenz $1373 - 1268 = 105$ zu betrachten, und da diese durch 7 teilbar ist, so ist es auch 13734.

2) Für den Modul 13 ist $1 \equiv -12$, $10 \equiv -3$, also

$$P \equiv -12a - 3b \equiv -3(b + 4a) \pmod{13},$$

allgemeiner

$$P \equiv -3[b + (4 + 13k)a] \pmod{13}.$$

Nach dieser Formel ist 1794 durch 13 teilbar, wenn

$$179 + 16 = 195$$

es ist; das ist aber der Fall, denn $19 + 20 = 39$ ist durch 13 teilbar.

3) Für den Modul 19 ist $1 \equiv -18$, $10 \equiv -9$, also

$$P \equiv -18a - 9b \equiv -9(b + 2a) \pmod{19}.$$

Bei Anwendung der in dieser Formel enthaltenen Regel bildet man aus 4389 zunächst $438 + 18 = 456$, dann $45 + 12 = 57$, und da letztere Zahl durch 19 teilbar ist, so ist es auch 4389.

III. Man kann auch

$$P = a + 100b$$

annehmen, wo a die aus den Einern und Zehnern gebildete und b die Zahl ist, die aus P bei Fortlassung der Einer und Zehner entsteht. Die Koeffizienten 1 und 100 lassen sich für gewisse Divisoren durch Reste ersetzen, welche zu bequemen Teilbarkeitsregeln führen (Hill, De factoribus numerorum compositorum dignoscendis. Crelles Journal XI, S. 251 ff.).

Beispiele. 1) Da $100 \equiv 2 \pmod{7}$ ist, so ist

$$(1) \quad P \equiv a + 2b \equiv a + (2 + 7k)b \pmod{7}.$$

Es ist aber auch $1 \equiv -6$, $100 \equiv 2$, also

$$(2) \quad P \equiv -6a + 2b \equiv 2(b - 3a) \pmod{7}.$$

Wenn man nach diesen beiden Formeln, von denen die erste schon im Talmud angegeben ist (vergl. G. Wertheim, Die Arithmetik des Elia Misrachi, S. 16), die Zahl 9268 untersucht, so liefert die erste die Zahlen

$$68 + 184 = 252, \quad 52 + 4 = 56,$$

die zweite

$$92 - 204 = -112, \quad 112 = 1 - 36 = -35,$$

jede zeigt also sofort, daß 9268 durch 7 teilbar ist.

2) Aus $100 \equiv 1 \pmod{11}$ folgt

$$P \equiv a + b \pmod{11}.$$

Nach dieser Formel erhält man z. B.

$$35781 \equiv 357 + 81 \equiv 438 \equiv 4 + 38 \equiv 42 \equiv 9 \pmod{11},$$

die Zahl 35781 giebt also bei der Division durch 11 den Rest 9.

3) Es ist $100 \equiv -4 \pmod{13}$, also

$$P \equiv a - 4b \text{ oder auch } P \equiv -(4b - a) \pmod{13}.$$

Danach ist

$$3588 \equiv -(140 - 88) \equiv -52 \equiv 0 \pmod{13},$$

$$35781 \equiv -(1428 - 81) \equiv -1347 \equiv + (52 - 47) \equiv 5 \pmod{13}.$$

4) Da $100 \equiv -2 \pmod{17}$ ist, so ist

$$P \equiv (a - 2b) \text{ oder auch } P \equiv -(2b - a) \pmod{17}.$$

P ist also durch 17 teilbar, wenn $a - 2b$ oder (falls $a - 2b$ negativ sein sollte) $2b - a$ es ist. Die Anwendung dieser

Regel auf die Zahl 39 542 führt zu den Zahlen

$$790 - 42 = 748, \quad 14 - 48 = -34,$$

39 542 ist also durch 17 teilbar.

IV. Es werde endlich

$$P = a + 1000b$$

gesetzt, wo also a eine dreistellige Zahl ist. Da nun

$$1000 \equiv -1 \pmod{7, \text{ mod. } 11, \text{ mod. } 13}$$

ist, so ergibt sich für jeden dieser drei Moduln

$$P \equiv a - b \equiv -(b - a).$$

Diese Formel enthält Teilbarkeitsregeln für 7, 11, 13, die sich leicht in Worten ausdrücken lassen.

V. Will man nicht bloß wissen, ob die Zahl

$$P = a_0 + 10a_1 + 10^2a_2 + \dots$$

durch m teilbar ist, sondern soll auch der Rest der Division von P durch m gefunden werden, so wähle man eine Potenz von 10, welche für m als Divisor einen recht kleinen Rest r liefert. Es sei

$$10^x \equiv r \pmod{m},$$

also $10^x - r$ durch m teilbar. Da nun $10^x - r$ in jede Zahl $10^{nx} - r^n$, in welcher n eine ganze positive Zahl ist, aufgeht, so wird jede der Zahlen

$$10^x - r, \quad 10^{2x} - r^2, \quad 10^{3x} - r^3, \dots$$

durch m teilbar sein. Wenn nun der Kürze wegen

$$\begin{aligned} A_0 &= a_0 + 10a_1 + 10^2a_2 + \dots + 10^{x-1}a_{x-1} \\ A_1 &= a_x + 10a_{x+1} + 10^2a_{x+2} + \dots + 10^{x-1}a_{2x-1} \\ A_2 &= a_{2x} + 10a_{2x+1} + 10^2a_{2x+2} + \dots + 10^{x-1}a_{3x-1} \\ &\dots \dots \dots \end{aligned}$$

gesetzt wird, so kann man

$$\begin{aligned} P &= A_0 + (10^x - r)A_1 + (10^{2x} - r^2)A_2 + \dots \\ &\quad + rA_1 \quad \quad \quad + r^2A_2 + \dots \end{aligned}$$

schreiben, und da jede der in Klammern stehenden Größen durch m teilbar ist, so ergibt sich

$$P \equiv A_0 + rA_1 + r^2A_2 + \dots \pmod{m}.$$

Anwendungen. Da $10^2 \equiv 2 \pmod{7}$, $10^2 \equiv 1 \pmod{11}$, $10^2 \equiv -1 \pmod{13}$, $10^2 \equiv -2 \pmod{17}$ ist, so erhalten wir

- (1) $P \equiv (a_0 + 10a_1) + 2(a_2 + 10a_3) + 4(a_4 + 10a_5) + (a_6 + 10a_7) + 2(a_8 + 10a_9) + 4(a_{10} + 10a_{11}) + \dots \pmod{7},$
- (2) $P \equiv (a_0 + 10a_1) + (a_2 + 10a_3) + \dots \pmod{11},$
- (3) $P \equiv (a_0 + 10a_1 + 10^2a_2) - (a_3 + 10a_4 + 10^2a_5) + \dots \pmod{13},$
- (4) $P \equiv (a_0 + 10a_1) - 2(a_2 + 10a_3) + 4(a_4 + 10a_5) - 8(a_6 + 10a_7) + \dots \pmod{17}.$

Nach diesen leicht in Worte zu kleidenden Regeln ergibt sich z. B.

$$\begin{aligned} 25689 &\equiv 89 + 112 + 8 \equiv 209 \equiv 9 + 4 \equiv 6 \pmod{7}, \\ 25689 &\equiv 89 + 56 + 2 \equiv 147 \equiv 47 + 1 \equiv 4 \pmod{11}, \\ 25689 &\equiv 689 - 25 \equiv 664 \equiv 1 \pmod{13}, \\ 25689 &\equiv 89 - 112 + 8 \equiv -15 \equiv 2 \pmod{17}. \end{aligned}$$

(Vergl. die Arbeit von Eduard Grohmann in der Zeitschrift für das Realschulwesen XVII, 12.)

§. 30.

Aufgaben.

Beweise folgende Sätze: I. Lautet eine Zahl a mit umgekehrter Ziffernfolge b , so ist $a - b$ immer durch 9 teilbar, $a + b$ aber nur dann, wenn a es ist.

II. Unter derselben Voraussetzung ist bei gerader Anzahl der Ziffern $a + b$, bei ungerader Anzahl $a - b$ durch 11 teilbar. Im ersten Falle ist es auch $a - b$ und im zweiten $a + b$, wenn a es ist.

III. Eine sechsstellige dekadische Zahl, welche mit zweimal 3 Ziffern in derselben Reihenfolge geschrieben wird, also die Form $abcabc$ hat, ist durch 7, 11 und 13 teilbar.

IV. Das Quadrat jeder ungeraden Zahl ist $\equiv 1 \pmod{8}$.

V. Die dritte Potenz jeder Zahl ist $\equiv 0$ oder $\equiv \pm 1 \pmod{9}$.

VI. Eine im Elfersystem geschriebene Zahl ist durch 2 oder 5 oder 10 teilbar, wenn ihre Quersumme durch 2 oder 5 oder 10 teilbar ist.

VII. Die im Elfersystem geschriebene Zahl ... *edcba* ist $\equiv a - b + c - d + e - \dots \pmod{3}$.

VIII. Die Zahl $2^{2^n} - 1$ ist für jeden Wert von n durch 3 teilbar.

IX. Ebenso ist $2^{2^n} - 1$ für jeden Wert von n durch 7 teilbar.

X. Ebenso ist $2^{2^n} - 1$ für jeden Wert von n durch 3 und durch 5, also durch 15 teilbar.

XI. Die Zahl $2^{2^n+1} + 1$ ist für jeden Wert von n durch 3 teilbar.

XII. Wenn a prim zu b und $a + b$ eine gerade Zahl ist, so ist das Produkt $ab(a + b)(a - b)$ durch 24 teilbar (Leonardo Pisano, Bd. II, S. 264).

Weitere Aufgaben:

XIII. Für welche Zahlensysteme gilt die Regel: Eine Zahl ist durch die Primzahl p teilbar, wenn ihre Quersumme es ist?

XIV. In welchen Zahlensystemen gilt für 7 die Teilbarkeitsregel, die im dekadischen System für 11 gilt?

XV. Das Produkt $1.2.3\dots 40$ in seine Primfaktoren zu zerlegen.

Man erhält

$$1.2.3\dots 40 = 2^{38}.3^{18}.5^9.7^5.11^3.13^3.17^2.19^2.23.29.31.37.$$

XVI. Auf wieviel Nullen endigt das Produkt $1.2.3\dots 10\,000$?
Auf

$$2000 + 400 + 80 + 16 + 3 = 2499 \text{ Nullen.}$$

XVII. Es soll gezeigt werden, daß

$$2620 = 2^2.5.131 \quad \text{und} \quad 2924 = 2^2.17.43$$

befreundete Zahlen sind.

XVIII. Beweise, daß die Zahl $p^\alpha q^\beta r^\gamma \dots$ auf

$$\frac{1}{2} + \frac{1}{2} (\alpha + 1)(\beta + 1)(\gamma + 1) \dots$$

oder auf

$$\frac{1}{2} (\alpha + 1)(\beta + 1)(\gamma + 1) \dots$$

Arten als Produkt von je zwei Faktoren dargestellt werden kann, je nachdem sie eine Quadratzahl ist oder nicht.

XIX. Beweise, daß 224 in nicht weniger als 7 aufeinander folgende Zahlen zerfällt werden kann.

XX. Es soll $2100 = 2^2 \cdot 3 \cdot 5^2 \cdot 7$ auf alle möglichen Arten als Produkt von je zwei Faktoren dargestellt werden, die prim zu einander sind.

$$1. 2100 = 3 \cdot 700 = 4 \cdot 525 = 7 \cdot 300 = 12 \cdot 175 = 25 \cdot 84 \\ = 28 \cdot 75 = 21 \cdot 100.$$

XXI. Beweise, daß die Zahl $p_1^{\alpha} p_2^{\beta} \dots p_k^{\gamma}$, wenn $p_1, p_2, \dots, p_k$ ungleiche Primzahlen sind, auf 2^{k-1} Arten als Produkt von je zwei Faktoren dargestellt werden kann, die prim zu einander sind.

§. 31.

Berechnung des Osterfestes.

Das Datum, auf welches der Ostersonntag fällt, wird nach Gauss (Werke, Bd. VI, S. 78) auf folgende Weise berechnet:

Es ergebe die Division

der Jahrzahl	durch 19	den Rest	a
" "	" 4	" "	b
" "	" 7	" "	c
" Zahl $19a + M$	" 30	" "	d
" " $2b + 4c + 6d + N$	" 7	" "	e ;

dann fällt der Ostersonntag auf den $(22 + d + e)^{\text{ten}}$ März oder den $(d + e - 9)^{\text{ten}}$ April.

M und N sind Zahlen, die im Julianischen Kalender auf immer, im Gregorianischen allemal wenigstens auf 100 Jahre unveränderliche Werte haben, und zwar ist in jenem $M = 15$, $N = 6$. Im Gregorianischen Kalender findet man die Werte von M und N für das Jahrhundert von $100k$ bis $100k + 99$ auf folgende Weise: Es sei p die größte ganze Zahl, die in dem Bruche $\frac{k}{3}$ enthalten ist, ebenso q die größte ganze Zahl, welche $\frac{k}{4}$ enthält; dann ist M der Rest der Division von $15 + k - p - q$ durch 30, N der Rest der Division von $4 + k - q$ durch 7.

Von der oben gegebenen Regel finden im Gregorianischen Kalender nur folgende zwei Ausnahmen statt:

1. Ergiebt die Rechnung für den Ostersonntag den 26. April, so wird dafür stets der 19. April genommen.

2. Gibt die Rechnung $d = 28$, $e = 6$ und ist zugleich der Rest der Division von $11M + 11$ durch 30 kleiner als 19, so fällt der Ostersonntag nicht, wie aus der Rechnung folgen würde, auf den 25., sondern auf den 18. April.

Aufgabe I. Auf welches Datum fiel der Ostersonntag des Jahres 1895?

Da hier $k = 18$ ist, so ergibt sich

$$p = E\left(\frac{18}{3}\right) = 6, \quad q = E\left(\frac{18}{4}\right) = 4,$$

also ist

$$M = 15 + 18 - 10 = 23 \equiv 23 \pmod{30},$$

$$N = 4 + 18 - 4 = 18 \equiv 4 \pmod{7},$$

$$M = 23, \quad N = 4.$$

Weiter folgt

$$1895 \equiv 14 \pmod{19}, \quad a = 14$$

$$1895 \equiv 3 \pmod{4}, \quad b = 3$$

$$1895 \equiv 5 \pmod{7}, \quad c = 5$$

$$19 \cdot 14 + 23 = 289 \equiv 19 \pmod{30}, \quad d = 19$$

$$6 + 20 + 114 + 4 = 144 \equiv 4 \pmod{7}, \quad e = 4,$$

also fiel der Ostersonntag, da $19 + 4 - 9 = 14$ ist, auf den 14. April.

Aufgabe II. In welchen Jahren des 20. Jahrhunderts fällt der Ostersonntag auf den 1. April?

Für das 20. Jahrhundert ist $M = 24$, $N = 5$, und wenn $d + e - 9 = 1$ sein soll, muß $d + e = 10$ sein, also d zwischen 0 und 10 liegen, während e seiner Definition nach zwischen 0 und 6 liegt. Nun kann a jeden der 19 Werte 0, 1, 2, ..., 18 haben, und für jeden derselben liefert die Definition von d einen bestimmten Wert von d . Die folgende Tabelle giebt die zwischen 0 und 10 liegenden Werte von d mit den zugehörigen Werten von a :

$a \dots$	2	4	7	10	13	15	18
$d \dots$	2	10	7	4	1	9	6

Da $d + e = 10$ und $e \leq 6$ sein muß, so sind die Fälle $d = 2$ und $d = 1$ auszuschliessen. Es sei nun erstens $a = 4$, $d = 10$. Dieser Wert von a entspricht den Jahren

1904,	und dafür ergibt sich	$b = 0, c = 0, e = 2,$
1923,	" " "	$b = 3, c = 5, e = 0,$
1942,	" " "	$b = 2, c = 3, e = 4,$
1961,	" " "	$b = 1, c = 1, e = 1,$
1980,	" " "	$b = 0, c = 6, e = 5,$
1999,	" " "	$b = 3, c = 4, e = 3.$

Es ist also nur für das Jahr 1923 $d + e = 10$.

Zweitens sei $a = 7, d = 7$. Dieser Wert von a entspricht den Jahren

1907,	und für diese folgt	$b = 3, c = 3, e = 2,$
1926,		$b = 2, c = 1, e = 6,$
1945,		$b = 1, c = 6, e = 3,$
1964,		$b = 0, c = 4, e = 0,$
1983,		$b = 3, c = 2, e = 5.$

Also ist im Jahre 1945 $d + e = 10$.

Für die den Werten $a = 10, d = 4$ entsprechenden Jahre 1910, 1929, ... ergibt sich $e < 6$, also kann $d + e$ nicht $= 10$ sein; dieser Fall scheidet somit aus.

Drittens sei $a = 15, d = 9$. Dann ergibt die Rechnung, daß $d + e = 10$ im Jahre 1934 ist.

Viertens liefert der Fall $a = 18, d = 6$ noch das Jahr 1956.

Der Ostersonntag fällt also nur in den vier Jahren des 20. Jahrhunderts 1923, 1934, 1945, 1956 auf den 1. April.

§. 32.

Umformung einer Kongruenz.

Es ist oft von Nutzen, eine Kongruenz

$$a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots + a_n \equiv 0 \pmod{m}$$

dadurch auf eine andere Form zu bringen, daß man jeden ihrer Koeffizienten $a_0, a_1, \dots, a_n$ durch einen seiner Reste für den Modul m ersetzt. Daß diese Umformung statthaft ist, geht aus den Sätzen des §. 27 hervor. Wird z. B. in der Kongruenz

$$35x^4 + 38x^3 + 40x^2 + 17x + 60 \equiv 0 \pmod{19}$$

jeder Koeffizient durch seinen absolut kleinsten Rest ersetzt, so

ergiebt sich

$$- 3x^4 + 2x^3 - 2x + 3 \equiv 0 \pmod{19}.$$

Man kann jetzt weiter solche Reste der Koeffizienten nehmen, welche durch 3, den Koeffizienten der höchsten Potenz von x , teilbar sind. Man erhält

$$- 3x^4 + 21x^3 - 21x + 3 \equiv 0 \pmod{19},$$

und da 3 prim zu 19 ist, so ist diese Kongruenz gleichbedeutend mit

$$x^4 - 7x^3 + 7x - 1 \equiv 0 \pmod{19}.$$

Wir haben also die vorgelegte Kongruenz in eine andere verwandelt, in welcher die höchste Potenz der Unbekannten den Koeffizienten 1 hat, ein Resultat, das sich freilich, wie wir im folgenden Kapitel sehen werden, nicht immer erreichen läßt.

§. 33.

Wurzeln von Kongruenzen.

Wenn jeder der Koeffizienten $a_0, a_1, \dots, a_n$ der Kongruenz

$$a_0 x^n + a_1 x^{n-1} + \dots + a_n \equiv 0 \pmod{m}$$

durch den Modul m teilbar ist, so wird die Kongruenz durch jeden Wert von x befriedigt. In diesem Falle nennt man sie eine identische Kongruenz. Die Kongruenz ist unmöglich, d.h. es giebt keinen Wert von x , der ihr genügt, wenn alle Koeffizienten, mit Ausnahme von a_n , durch m teilbar sind.

Wir nehmen jetzt an, es sei weder das eine, noch das andere der Fall, und bezeichnen mit x_1 eine Zahl, durch deren Einsetzung an die Stelle von x die linke Seite der Kongruenz durch m teilbar wird. Dann wird x_1 eine Wurzel der Kongruenz genannt. So ist 5 eine Wurzel der Kongruenz

$$3x - 2 \equiv 0 \pmod{13},$$

da $3 \cdot 5 - 2 = 13$ durch 13 teilbar ist.

Wenn x_1 Wurzel einer Kongruenz ist, welche den Modul m hat, so genügt der Kongruenz auch jede der unendlich vielen Zahlen, welche $\equiv x_1 \pmod{m}$ sind, also jede Zahl $x_1 + km$, wo k völlig unbestimmt bleibt. Die oben genannte Kongruenz wird z. B. durch jede Zahl $5 + 13k$ befriedigt, wo k jede ganze Zahl

sein darf. Alle diese kongruenten Zahlen sieht man aber nur als eine einzige Wurzel an. Die verschiedenen Wurzeln einer Kongruenz bestimmen, heisst die inkongruenten Zahlen suchen, welche derselben genügen.

Es kann auch nach der Auflösung einer Kongruenz oder eines Systems von Kongruenzen mit mehreren Unbekannten gefragt werden. Darunter versteht man die der Aufgabe genügenden zusammen gehörenden Werte $x_1, y_1, \dots$ der Unbekannten.

So hat z. B. die Kongruenz

$$13x - 7y + 6 \equiv 0 \pmod{19}$$

die Auflösung

$$x_1 \equiv 3, \quad y_1 \equiv 1 \pmod{19},$$

ebenso die Auflösung

$$x_2 \equiv 5, \quad y_2 \equiv 2 \pmod{19}.$$

Die Kongruenzen

$$\left. \begin{array}{l} 25x - 17y + 11 \equiv 0 \\ 16x + 9y + 12 \equiv 0 \end{array} \right\} \pmod{26}$$

haben die Auflösung

$$x_1 \equiv 3, \quad y_1 \equiv 2 \pmod{26}.$$

Wenn man in der Kongruenz

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n \equiv 0 \pmod{m},$$

in der $a_0, a_1, \dots, a_n$ ganze Zahlen bezeichnen, während n eine positive ganze Zahl ist, für x alle Glieder eines vollständigen Restsystems mod. m einsetzt, so erhält man nach den Sätzen des §. 27 die Reste aller Werte, welche $f(x)$ annehmen kann. Diese Bemerkung gestattet es, die sämtlichen Wurzeln einer solchen Kongruenz durch Probieren zu finden.

Beispiele.

$$\text{I. } f(x) = 3x - 5 \equiv 0 \pmod{6}.$$

Da $f(x)$ für $x = 0, 1, 2, 3, 4, 5$ beziehungsweise mod. 6 $\equiv -5, -2, 1, 4, 1, 4$ wird, also nicht den Rest 0 liefert, so ist die Kongruenz unmöglich.

$$\text{II. } f(x) = 3x - 5 \equiv 0 \pmod{7}.$$

$f(x)$ wird für $x = 0, 1, 2, 3, 4, 5, 6$ für den Modul 7 be-

ziehungsweise $\equiv -5, -2, 1, 4, 0, 3, 6$. Folglich hat die Kongruenz eine Wurzel, nämlich $x \equiv 4 \pmod{7}$.

$$\text{III. } f(x) = 3x - 6 \equiv 0 \pmod{9}.$$

$f(x)$ wird für $x = 0, 1, 2, 3, 4, 5, 6, 7, 8$ beziehungsweise $\equiv -6, -3, 0, 3, 6, 0, 3, 6, 0 \pmod{9}$. Folglich hat die Kongruenz die drei Wurzeln $x \equiv 2, 5, 8 \pmod{9}$.

$$\text{IV. } f(x) = x^3 - 2x^2 + 6 \equiv 0 \pmod{9}.$$

Für $x = 0, 1, 2, 3, 4, 5, 6, 7, 8$ ist beziehungsweise $f(x) \equiv 6, 5, 6, 6, 2, 0, 6, 8, 3 \pmod{9}$. Folglich hat die Kongruenz eine Wurzel, nämlich $x \equiv 5 \pmod{9}$.

Drittes Kapitel.

Kongruenzen ersten Grades.

§. 34.

Die Kongruenz ersten Grades mit einer Unbekannten.
Anzahl ihrer Wurzeln.

Jede Kongruenz ersten Grades mit einer Unbekannten kann
auf die Form

$$ax \equiv b \pmod{m}$$

gebracht werden; darin bezeichnen a, b, m gegebene ganze Zahlen,
und nach §. 32 kann man annehmen, jede der Zahlen a, b sei
kleiner als der Modul m .

Nun haben die am Ende des §. 33 gegebenen Beispiele gezeigt,
daß nicht jede Kongruenz $ax \equiv b \pmod{m}$ möglich ist,
ebenso daß von den möglichen Kongruenzen dieser Form nicht
die eine ebenso viele Wurzeln besitzt wie die andere. Es liegt
uns also zunächst ob, zu bestimmen, welche Kongruenzen ersten
Grades unmöglich sind, d. h. überhaupt keine Wurzeln besitzen.
Diese Frage beantwortet der Sache nach der schon von Bháscara¹⁾ ausgesprochene

Lehrsatz I. Die Kongruenz $ax \equiv b \pmod{m}$ ist unmöglich,
wenn der grösste gemeinschaftliche Divisor d von a und m nicht auch in b aufgeht.

Beweis. Da vorausgesetzt wird, daß $ax - b$ ein Vielfaches,
etwa das k fache von m sei, so ist

$$ax - km = b.$$

¹⁾ Algebra with Arithmetic and Mensuration from the Sanscrit of
Brahmegupta and Bháscara. Translated by Colebrooke, S. 156.

Nun ist die linke Seite ein Vielfaches von d , da d ein Divisor von a wie auch von m sein soll; folglich ist die Gleichung und daher die mit derselben identische Kongruenz nur möglich, wenn auch die rechte Seite durch d teilbar ist, d. h. wenn d in b aufgeht.

Nach diesem Satze ist z. B. die Kongruenz $6x \equiv 7 \pmod{12}$ unmöglich, da 6 nicht in 7 aufgeht.

Wenn die in dem vorhergehenden Satze für die Möglichkeit der Kongruenz ersten Grades ausgesprochene Bedingung erfüllt ist, also der größte gemeinschaftliche Divisor d von a und m in b aufgeht, so können wir d wegheben. Dadurch gelangen wir zu einer Kongruenz, deren Modul prim zum Koeffizienten der Unbekannten ist. Wird nämlich

$$a = d\alpha, \quad m = d\mu, \quad b = d\beta$$

vorausgesetzt, so sind α und μ relative Primzahlen, und die Gleichung $ax = b + mk$, welche mit der vorgelegten Kongruenz $ax \equiv b \pmod{m}$ identisch ist, geht über in $\alpha x = \beta + \mu k$, führt also zu der Kongruenz $\alpha x \equiv \beta \pmod{\mu}$, welche durch dieselben Werte wie die vorgelegte befriedigt wird. Von dieser neuen Kongruenz gilt der

Lehrsatz II. Wenn a prim zu m ist, so hat die Kongruenz $ax \equiv b \pmod{m}$ stets eine, aber auch nur eine Wurzel.

Beweis. Von den Produkten

$$a, \quad 2a, \quad 3a, \quad \dots, \quad (m-1)a$$

kann keines für den Modul m den Rest Null liefern; denn wäre eins derselben, etwa ka , durch m teilbar, so müßte, da a prim zu m ist, k durch m teilbar sein (§. 17, Satz I); das ist aber unmöglich, da $k < m$ ist.

Ferner sind jene Produkte für den Modul m inkongruent; denn wäre $ka \equiv k'a \pmod{m}$, so müßte nach §. 27, V auch $k \equiv k' \pmod{m}$ sein, während zwei Zahlen der Reihe

$$1, \quad 2, \quad 3, \quad \dots, \quad m-1$$

für diesen Modul nicht kongruent sein können. Da somit jene $m-1$ Produkte für den Modul m verschiedene Reste geben, und da der Rest Null ausgeschlossen ist, so müssen ihre Reste in irgend einer Reihenfolge mit den Zahlen $1, 2, 3, \dots, m-1$ übereinstimmen, dergestalt, daß jedes Produkt einer, aber auch nur

einer dieser Zahlen kongruent ist. Unter den letzteren befindet sich auch b . Es giebt also eine einzige Zahl x , welche, mit a multipliziert, für den Modul m den Rest b liefert, d. h. der gegebenen Kongruenz genügt.

Beispiel. Die Kongruenz $7x \equiv 3 \pmod{15}$ hat nur die eine Wurzel $x \equiv 9 \pmod{15}$.

Zusatz. Die Kongruenz $ax \equiv b \pmod{p}$, deren Modul p eine Primzahl ist, hat immer eine, aber auch nur eine Wurzel.

Wenn wir die Kongruenz $adx \equiv bd \pmod{md}$, wo a und m als teilerfremd vorausgesetzt werden, durch d heben, so besitzt die erhaltene Kongruenz $ax \equiv b \pmod{m}$ nach dem vorhergehenden Lehrsatz eine einzige Wurzel, indem die unzählig vielen Werte, die ihr genügen und die sämtlich auch die erste Kongruenz befriedigen, nach dem Modul m kongruent sind. Damit ist aber nicht gesagt, daß sie auch für den Modul md kongruent sein werden, d. h. daß auch die Kongruenz $adx \equiv bd \pmod{md}$ nur eine Wurzel besitzt. Es besteht im Gegenteil der

Lehrsatz III. Die Kongruenz $adx \equiv bd \pmod{md}$ hat, wenn d der grösste gemeinschaftliche Divisor von ad und md ist, so daß also a und m teilerfremd sind, d inkongruente Wurzeln.

Beweis. Die Kongruenz $ax \equiv b \pmod{m}$, in welche die vorgelegte Kongruenz durch Division mit d übergeht, hat nach Lehrsatz II. nur eine Wurzel, die wir mit x_1 bezeichnen wollen. Die gegebene Kongruenz hat dann die d Wurzeln

$$x_1, x_1 + m, x_1 + 2m, \dots, x_1 + (d - 1)m,$$

die (zwar für den Modul m kongruent, aber) für den Modul md offenbar inkongruent sind.

Beispiel. Die Kongruenz $27x \equiv 18 \pmod{36}$ geht durch Division mit 9 über in

$$3x \equiv 2 \pmod{4}.$$

Diese Kongruenz hat die eine Wurzel $x \equiv 2 \pmod{4}$, folglich hat die gegebene Kongruenz die neun Wurzeln

$$\begin{aligned} x_1 &\equiv 2, & x_2 &\equiv 2 + 4 \equiv 6, & x_3 &\equiv 2 + 8 \equiv 10, \\ x_4 &\equiv 2 + 12 \equiv 14, & x_5 &\equiv 2 + 16 \equiv 18, & x_6 &\equiv 2 + 20 \equiv 22, \\ x_7 &\equiv 2 + 24 \equiv 26, & x_8 &\equiv 2 + 28 \equiv 30, & x_9 &\equiv 2 + 32 \equiv 34 \pmod{36}. \end{aligned}$$

§. 35.

Auflösung der Kongruenz ersten Grades mit einer Unbekannten.

Wir haben im vorigen Paragraphen gesehen, daß die Kongruenz

$$ax \equiv b \pmod{m}$$

nur möglich ist, wenn der größte gemeinschaftliche Divisor von a und m auch in b aufgeht, und daß sie dann in jedem Falle so viele für den Modul m inkongruente Wurzeln besitzt, als dieser Divisor Einheiten enthält. Wir gehen jetzt dazu über, diese Wurzeln zu bestimmen. Dabei können wir $a < m$ und $b < m$ voraussetzen; denn wäre diese Bedingung nicht erfüllt, so könnten wir statt der Zahlen a, b ihre kleinsten Reste für den Modul m nehmen. Ebenso dürfen wir annehmen, a sei prim zu m ; denn ein etwa vorhandener gemeinschaftlicher Divisor beider Zahlen ließe sich nach §. 34 durch Division entfernen.

Zur Auflösung der vorgelegten Kongruenz können wir nun zunächst das in §. 33 dargelegte Probiervverfahren anwenden. Am zweckmäßigsten geschieht dies auf folgende Weise: Man bilde die Reihe

$$b, \quad b + m, \quad b + 2m, \quad b + 3m, \dots$$

und nehme die kleinste dieser Zahlen, die durch a teilbar ist. Ist $b + km$ diese Zahl, so ist

$$\frac{b + km}{a} = x_1$$

die gesuchte Wurzel. Es ist nämlich

$$ax_1 = b + km,$$

also

$$ax_1 \equiv b \pmod{m}.$$

Beispiele.

$$\text{I. } 7x \equiv 1 \pmod{15}.$$

In der Reihe

$$1, \quad 16, \quad 31, \quad 46, \quad 61, \quad 76, \quad 91, \dots$$

ist 91 die kleinste durch 7 teilbare Zahl; folglich ist $\frac{91}{7} = 13$ die gesuchte Wurzel.

Anmerkung. Man kann die Reihe auch nach rückwärts fortsetzen, also ein durch a teilbares Glied der Reihe

$$\dots, b - 3m, b - 2m, b - m, b, b + m, b + 2m, b + 3m, \dots$$

suchen. Auf diese Weise kommt man oft schneller zum Ziel. Im vorhergehenden Beispiel würde die Reihe

$$\dots, -29, -14, 1, 16, 31, \dots$$

sein, und wir erhielten die Wurzel

$$\frac{-14}{7} = -2 \equiv 13 \pmod{15}.$$

$$\text{II. } 15x \equiv 11 \pmod{23}.$$

In der Reihe

$$11, 34, 57, 80, 103, 126, 149, 172, 195, \dots$$

ist 195 das kleinste durch 15 teilbare Glied; also ist

$$\frac{195}{15} = 13$$

die gesuchte Wurzel.

Ein zweites Verfahren besteht darin, daß man durch Anwendung der Sätze über die Verbindung der Kongruenzen (§. 27) den Koeffizienten von x auf die Einheit reduziert. Oft geschieht dies dadurch, daß man einfach eine Zahl k bestimmt, für welche ak entweder $\equiv +1$ oder $\equiv -1 \pmod{p}$ ist, und da a prim zu m ist, so ist diese Bedingung stets erfüllbar. Durch Multiplikation der vorgelegten Kongruenz mit k erhält man dann

$$akx \equiv bk \pmod{m},$$

also entweder

$$x \equiv bk \text{ oder } x \equiv -bk \pmod{m}.$$

Man übersehe nicht, daß dieses Verfahren, so bequem seine Anwendung in vielen Fällen auch ist, doch nicht den Namen einer Auflösungsmethode verdient, da es schon die Auflösung einer Kongruenz ersten Grades benutzt. (Siehe die betreffende Tabelle des Anhangs.)

Beispiele.

$$\text{I. } 17x \equiv 11 \pmod{19}.$$

$$153x \equiv 99,$$

$$x \equiv 4.$$

oder auch

$$\begin{aligned} -2x &\equiv -8, \\ x &\equiv 4 \pmod{19}. \end{aligned}$$

$$\begin{aligned} \text{II. } 3x &\equiv 2 \pmod{25}, \\ 24x &\equiv 16, \\ -x &\equiv 16, \\ x &\equiv -16 \equiv 9 \pmod{25}. \end{aligned}$$

$$\begin{aligned} \text{III. } 15x &\equiv 11 \pmod{23}, \\ -8x &\equiv -12, \\ 2x &\equiv 3 \equiv -20, \\ x &\equiv -10 \equiv 13 \pmod{23}, \end{aligned}$$

oder auch

$$\begin{aligned} 8x &\equiv 12, \\ 16x &\equiv 24, \\ 16x - 15x &\equiv 24 - 11, \\ x &\equiv 13 \pmod{23}. \end{aligned}$$

Bachets Auflösungsmethode. Die Kongruenz

$$ax \equiv b \pmod{m}$$

ist gleichbedeutend mit der Gleichung

$$ax = b + my,$$

in welcher a, b, m gegebene, x und y gesuchte ganze Zahlen bedeuten. Da diese Gleichung zwei Unbekannte x, y enthält, so ist sie unbestimmt, d. h. sie läßt im allgemeinen unendlich viele Lösungen zu. Man kann nämlich der einen Unbekannten jeden beliebigen Wert beilegen und dann mittels der Gleichung den zugehörigen Wert der anderen Unbekannten berechnen. Wenn man sich aber auf ganze und (wie es vielfach geschieht) positive Werte der Unbekannten beschränkt, so wird die Zahl der Lösungen verringert. Oft sind in den Aufgaben, die zu unbestimmten Gleichungen führen, noch Bedingungen angegeben, die sich zwar nicht in Gleichungen umsetzen lassen, aber doch die Zahl der Lösungen weiter verringern. Wenn z. B. verlangt wird, daß eine gesuchte Zahl eine gewisse Grenze nicht überschreiten soll, so werden alle jenseits dieser Grenze liegenden, sonst zulässigen Werte ausgeschlossen.

Um jetzt die Gleichung $ax = b + my$ in ganzen Zahlen zu lösen, dividieren wir mit a und erhalten

$$x = b_1 + m_1 y + \frac{\beta + \mu y}{a},$$

wo b_1 und m_1 die Quotienten, β und μ die Reste der Division von b und m durch a bezeichnen. Da nun x, y, b_1, m_1 ganze Zahlen sind, so muß auch $\frac{\beta + \mu y}{a}$ eine ganze Zahl sein, die wir mit z bezeichnen wollen. Aus

$$\frac{\beta + \mu y}{a} = z$$

erhalten wir

$$y = \frac{-\beta + az}{\mu}$$

und, wenn wir die Division mit μ in $-\beta$ und a ausführen und die Quotienten mit b_2 und m_2 , die Reste mit β_1 und μ_1 bezeichnen,

$$y = b_2 + m_2 z + \frac{\beta_1 + \mu_1 z}{\mu}.$$

Mit dem Bruche $\frac{\beta_1 + \mu_1 z}{\mu}$, der ebenfalls eine ganze Zahl sein muß, da y, z, b_2, m_2 ganze Zahlen sind, verfahren wir ebenso, wie wir mit $\frac{\beta + \mu y}{a}$ verfahren, und da die Brüche, zu denen wir auf diese Weise gelangen, immer kleinere Zahlen zu Nennern haben ($a > \mu > \dots$), so müssen wir endlich einen Bruch mit dem Nenner 1 erhalten. Die letzte Gleichung bestimmt dann die vorletzte der Unbekannten $x, y, z, \dots$ mittelst der (unbestimmt bleibenden) letzten, und durch eine Reihe von Substitutionen lassen sich rückwärts alle vorhergehenden Unbekannten, also zuletzt auch x durch dieselbe unbestimmte Größe ausdrücken.

Es ist vorteilhaft, in der Rechnung immer die absolut kleinsten Reste zu nehmen; man kommt dadurch am schnellsten zu einem Bruch mit dem Nenner 1.

Beispiel. Die Kongruenz $19x \equiv 8 \pmod{29}$ führt zu der Gleichung

$$19x = 8 + 29y.$$

Diese liefert der Reihe nach

$$x = 2y - \frac{9y - 8}{19} = 2y - z,$$

$$9y - 8 = 19z, y = \frac{19z + 8}{9} = 2z + 1 + \frac{z - 1}{9} = 2z + 1 + u,$$

$$z - 1 = 9u, z = 9u + 1,$$

und daraus folgt rückwärts

$$y = 19u + 3,$$

$$x = 29u + 5.$$

Die Kongruenz hat also die Wurzel $x \equiv 5 \pmod{29}$.

Wenn von vornherein eine Gleichung ersten Grades mit zwei Unbekannten vorliegt, so empfiehlt es sich häufig, erst die Gleichung durch die Kongruenz zu ersetzen, welche den kleinsten der Koeffizienten der Unbekannten zum Modul hat, die Kongruenz mittels §. 27 zu vereinfachen und dann die mit der vereinfachten Kongruenz gleichbedeutende Gleichung in der dargelegten Weise zu lösen.

Beispiele.

I. $17x = 2 + 65y.$

$$65y \equiv -2 \pmod{17},$$

$$-3y \equiv -2,$$

$$3y \equiv 2,$$

$$3y = 2 + 17z, \quad y = 1 + 6z - \frac{1+z}{3};$$

$$\frac{1+z}{3} = u, \quad z = 3u - 1;$$

$$y = 17u - 5, \quad x = 65u - 19.$$

II. $6259x - 2773y = 1.$

$$6259x \equiv 1 \pmod{2773},$$

$$713x \equiv 1,$$

$$713x = 1 + 2773z,$$

$$x = \frac{1 + 2773z}{713} = 4z - \frac{79z - 1}{713};$$

$$\frac{79z - 1}{713} = u, \quad z = \frac{713u + 1}{79} = 9u + \frac{2u + 1}{79};$$

$$\frac{2u + 1}{79} = v, \quad u = \frac{79v - 1}{2} = 39v + \frac{v - 1}{2};$$

$$\frac{v - 1}{2} = w, \quad v = 2w + 1.$$

$$u = 79w + 39,$$

$$z = 713w + 352,$$

$$x = 2773w + 1369,$$

$$y = 6259w + 3090.$$

Anmerkung I. Wenn man ein Wurzelpaar der Gleichung $ax + by = c$ auf irgend eine Weise (durch Erraten, Probieren

oder dergl.) gefunden hat, so ist es leicht, die allgemeine Lösung zu erhalten. Das gefundene Wurzelpaar sei ξ, η ; dann ist

$$ax + by = c$$

$$a\xi + b\eta = c,$$

folglich

$$a(x - \xi) + b(y - \eta) = 0,$$

oder

$$\frac{x - \xi}{y - \eta} = \frac{+b}{-a} = \frac{+bk}{-ak},$$

wo k jede ganze Zahl sein kann. Die allgemeine Lösung der Gleichung ist also

$$\begin{cases} x = \xi + bk \\ y = \eta - ak. \end{cases}$$

Beispiel. Die Gleichung $15x - 23y = 11$ wird durch die Werte $x = 13, y = 8$ befriedigt; ihre allgemeine Lösung ist daher

$$\begin{cases} x = 13 + 23k \\ y = 8 - 15k, \end{cases}$$

wo k jede ganze (positive oder negative) Zahl sein kann.

Anmerkung II. Aufgaben, welche zu unbestimmten Gleichungen ersten Grades führen und in ganzen positiven Zahlen gelöst werden sollen, werden — nicht ganz zutreffend — diophantische genannt. Der griechische Mathematiker Diophantus von Alexandria behandelt zwar in seiner Arithmetik¹⁾ vorwiegend (nicht ausschließlich) unbestimmte Aufgaben, aber er fordert immer nur Lösungen in rationalen, nicht in ganzen Zahlen. Die Lösung der Gleichung $ax = b + cy$ in ganzen Zahlen ist zwar schon um 500 v. Chr. den alten Indern²⁾ gelungen; aber die Leistungen dieses Volkes in der Mathematik sind erst im 19. Jahrhundert in Europa bekannt geworden. Hier hatte inzwischen Claude Gaspar Bachet de Méziriac, der berühmte Herausgeber des Diophant, die Aufgabe von neuem gelöst. Er setzt sein Verfahren, das später Euler (Algebra, Bd. II, Kap. I oder auch *Commentationes arithmeticae collectae*, Bd. I, S. 11) mit der ihm eigenen Klarheit dargelegt hat, und das oben mitgeteilt worden ist, in seinen „*Problèmes*

¹⁾ Deutsche Übersetzung von G. Wertheim. Leipzig 1890.

²⁾ Siehe die Anmerkung zu §. 62.

plaisans et delectables, qui se font par les nombres“ auseinander und zwar in der zweiten 1624 erschienenen Ausgabe, nachdem er es in der ersten Ausgabe (1612) nur angekündigt hatte. Weiter unten werden wir noch einige andere Auflösungsmethoden der Kongruenz ersten Grades mit einer Unbekannten, resp. der Gleichung ersten Grades mit zwei Unbekannten behandeln, für die ganze Zahlen gesucht werden sollen. (S. §. 45, 62, 78, 88, 94, 97.)

§. 36.

Zurückführung der Kongruenzen ersten Grades, deren Moduln zusammengesetzte Zahlen sind, auf solche mit Primzahlmoduln.

Wir nehmen an, der Modul der Kongruenz

$$(1) \quad ax \equiv b \pmod{m}$$

sei eine zusammengesetzte Zahl, $m = pn$, wo p eine Primzahl, n eine beliebige Zahl bezeichnet. Dann muß auch

$$(2) \quad ax \equiv b \pmod{p}$$

sein; denn da die Zahl $ax - b$ durch das Produkt pn teilbar sein soll, so muß sie auch durch jeden Faktor desselben, also durch p teilbar sein. Die Kongruenz (2) habe die Wurzel x_1 ; dann hat (1) die Wurzel $x_1 + py$, wofern für y ein passender Wert genommen wird. Um diesen Wert von y zu bestimmen, ersetzen wir in (1) x durch $x_1 + py$ und erhalten

$$ax_1 + apy \equiv b \pmod{m}$$

oder

$$apy \equiv b - ax_1 \pmod{pn}.$$

Da x_1 eine Wurzel von (2) ist, so ist $b - ax_1$ ein Vielfaches von p , etwa gleich cp , und daher geht die vorhergehende Kongruenz durch Division mit p über in

$$(3) \quad ay \equiv c \pmod{n}.$$

Diese Kongruenz dient zur Bestimmung von y .

Wenn nun n eine Primzahl ist, so ist die Lösung der Aufgabe beendet. Im entgegengesetzten Falle haben wir mit (3) ebenso zu verfahren, wie wir mit (1) verfahren sind, und auf

diese Weise können wir allmählich die Auflösung der Kongruenz ersten Grades, deren Modul eine zusammengesetzte Zahl ist, auf die von Kongruenzen zurückführen, von denen jede eine Primzahl zum Modul hat.

Beispiel (Gauss, Disquisitiones, 30). Um die Kongruenz

$$(1) \quad 19x \equiv 1 \pmod{140}$$

zu lösen, behandeln wir zunächst

$$(2) \quad 19x \equiv 1 \pmod{2}$$

und erhalten

$$x \equiv 1 \pmod{2},$$

d. h.

$$x = 1 + 2x'.$$

Wird dieser Wert von x in (1) eingesetzt, so folgt

$$19 + 38x' \equiv 1 \pmod{140}$$

oder

$$(3) \quad 19x' \equiv -9 \pmod{70}.$$

Auch diese Kongruenz lösen wir zunächst für den Modul 2, behandeln also

$$(4) \quad 19x' \equiv -9 \pmod{2}$$

und erhalten

$$x' \equiv 1 \pmod{2},$$

d. h.

$$x' = 1 + 2x''.$$

Für diesen Wert von x' geht (3) über in

$$19 + 38x'' \equiv -9 \pmod{70}$$

oder

$$(5) \quad 19x'' \equiv -14 \pmod{35}.$$

Diese Kongruenz lösen wir für den Modul 5, behandeln also

$$(6) \quad 19x'' \equiv -14 \pmod{5}$$

und erhalten

$$x'' \equiv 4 \pmod{5},$$

d. h.

$$x'' = 4 + 5x'''.$$

Für diesen Wert geht (5) über in

$$76 + 95x''' \equiv -14 \pmod{35}$$

oder

$$(7) \quad 19x''' \equiv -18 \pmod{7}.$$

Die Wurzel dieser Kongruenz ist

$$x''' \equiv 2 \pmod{7};$$

es ist also

$$x'' = 2 + 7x''',$$

und wir erhalten rückwärts schreitend

$$x'' = 14 + 35x''',$$

$$x' = 29 + 70x''',$$

$$x = 59 + 140x''',$$

also

$$x \equiv 59 \pmod{140}.$$

§. 37.

Anwendungen der Kongruenzen ersten Grades.

I. Aufgabe. Die Zahl 100 in zwei Teile zu zerlegen, von denen der erste bei der Division durch 5 den Rest 2, der zweite bei der Division durch 7 den Rest 4 giebt (Euler, Algebra, Bd. II, Kap. I, Nr. 6).

Der erste Teil wird von der Form $5x + 2$, der zweite von der Form $7y + 4$ sein; wir erhalten also die Gleichung

$$(5x + 2) + (7y + 4) = 100,$$

d. i. $5x + 7y = 94$, oder die Kongruenz

$$7y \equiv 94 \pmod{5},$$

deren Wurzel $y \equiv 2 \pmod{5}$ ist. Es ist also $y = 2 + 5k$, und durch Einsetzung dieses Wertes in die Gleichung

$$5x + 7y = 94$$

folgt $x = 16 - 7k$. Als die gesuchten Teile von 100 ergeben sich danach

$$5x + 2 = 82 - 35k,$$

$$7y + 4 = 18 + 35k.$$

Damit beide Teile positiv seien, darf k nur $= 0$ oder 1 oder 2 angenommen werden. Die Aufgabe läßt danach drei Lösungen zu, nämlich 82 und 18, 47 und 53, 12 und 88.

II. In einer Rechnung findet sich der Posten

$$*24 \text{ fl. } \dot{\text{a}} 1,9 * \mathcal{M} = \mathcal{M} * 38,08.$$

Da, wo das Zeichen * steht, sind die Ziffern unleserlich. Wie heißen diese Ziffern? [S. Wertheim, Elemente der Zahlen-theorie, Leipzig 1887, S. 43.]

Werden dieselben der Reihe nach mit x , y , z bezeichnet, so erhält man, wenn man auf Pfennige rechnet, die Gleichung

$$(24 + 100x)(190 + y) = 3808 + 10000z,$$

und daraus folgt leicht

$$y = -190 + 4 \cdot \frac{625z + 238}{25x + 6}.$$

Nun soll y eine der Zahlen 0, 1, 2, ..., 9 sein, daher muls

$$4 \cdot \frac{625z + 238}{25x + 6} < 200,$$

aber ≥ 190 , also

$$50 > \frac{625z + 238}{25x + 6} \geq 48$$

sein. Dieser Bruch kann daher nur die Werte 49 und 48 haben. Die Annahme

$$\frac{625z + 238}{25x + 6} = 49$$

liefert aber

$$625z + 238 = 1225x + 294,$$

führt also zu der Kongruenz

$$625z \equiv 56 \pmod{1225},$$

die nach §. 34, Lehrsatz I unmöglich ist. Wird weiter

$$\frac{625z + 238}{25x + 6} = 48$$

gesetzt, so ergibt sich der Reihe nach

$$\begin{aligned} 625z + 238 &= 1200x + 288, \\ 25z &= 48x + 2, \\ 48x &\equiv -2 \pmod{25}, \\ x &\equiv 1 \pmod{25}. \end{aligned}$$

Es ist also $x = 1 + 25k$, und damit x eine einstellige Zahl sei, ist $k = 0$ anzunehmen, so dafs wir $x = 1$ erhalten. Für diesen Wert wird $z = 2$, $y = 2$; der Posten lautet somit

$$124 \text{ fl. } \dot{\text{a}} \mathcal{M} 1,92 = 238,08 \mathcal{M}.$$

III. Ein gezahntes Rad mit 30 Zähnen greift in die Lücken eines zweiten Rades, das 41 Zähne hat, und zwar anfangs der erste Zahn des ersten Rades in die erste Lücke des zweiten. Wieviel Umdrehungen wird jedes gemacht haben, wenn der erste Zahn des ersten Rades in die zehnte Lücke des zweiten greift?

Nach x Umdrehungen des ersten und y des zweiten Rades soll

$$30x = 41y + 9$$

sein, und daraus folgt leicht

$$x = 41k - 12, \quad y = 30k - 9,$$

wo k unbestimmt bleibt.

IV. Wie bestimmt man aus $\frac{1}{6}$ und $\frac{1}{10}$ der Kreisperipherie $\frac{1}{15}$ derselben?

Die Gleichung

$$\frac{x}{6} + \frac{y}{10} = \frac{1}{15}$$

gibt, wenn man sich auf echte Brüche beschränkt, die vier Lösungen

$$\frac{1}{15} = \frac{1}{6} - \frac{1}{10} = \frac{2}{3} - \frac{3}{5} = \frac{2}{5} - \frac{1}{3} = \frac{9}{10} - \frac{5}{6}.$$

§. 38.

Zahlen, welche für gegebene Moduln $m_1, m_2, \dots, m_n$ gegebene Reste $r_1, r_2, \dots, r_n$ liefern.

Es soll eine Zahl x ermittelt werden, welche den Kongruenzen

$$x \equiv r_1 \pmod{m_1}, \quad x \equiv r_2 \pmod{m_2}, \quad \dots, \quad x \equiv r_n \pmod{m_n},$$

d. i. den Gleichungen

$$x = r_1 + m_1 y, \quad x = r_2 + m_2 z, \quad \dots, \quad x = r_n + m_n u$$

genügt, wo $y, z, \dots, u$ unbestimmte Zahlen bezeichnen. Eliminieren wir x aus den beiden ersten Gleichungen, setzen also

$$r_1 + m_1 y = r_2 + m_2 z,$$

so erhalten wir eine Gleichung mit den Unbekannten y und z , die nach §. 35 zu lösen ist. Wir können durch Benutzung des

auf diese Weise für y oder z erhaltenen Wertes einen neuen Ausdruck für x bilden, dessen Einsetzung in die dritte Gleichung die Bildung eines dritten Ausdrucks von x ermöglicht. So fortfahrend gelangen wir nach und nach zu einem Ausdruck für x , der allen gestellten Bedingungen genügt.

Beispiel. Welche Zahl giebt bei der Division durch 67, 15 und 7 beziehungsweise die Reste 10, 13 und 5?

Die gesuchte Zahl x soll den drei Gleichungen

$$x = 10 + 67y, \quad x = 13 + 15z, \quad x = 5 + 7u$$

genügen. Setzt man

$$10 + 67y = 13 + 15z,$$

so ergibt sich leicht

$$y = 15k - 6, \quad z = 67k - 27, \quad x = 1005k - 392,$$

wo k unbestimmt bleibt.

Weiter setzen wir

$$1005k - 392 = 5 + 7u$$

und erhalten

$$u = 1005l + 374, \quad x = 7035l + 2623,$$

wo l eine neue unbestimmt bleibende ganze Zahl bezeichnet. Es genügen also alle in dem Ausdruck $7035l + 2623$ enthaltenen ganzen Zahlen den gestellten Bedingungen.

Andere Lösung der Aufgabe. (Gauss, Disquisitiones 36.) Wir bestimmen eine Zahl t_1 , welche den Kongruenzen

$$t_1 \equiv 1 \pmod{m_1}, \quad t_1 \equiv 0 \pmod{m_2}, \dots, \quad t_1 \equiv 0 \pmod{m_n}$$

genügt. Ebenso ermitteln wir eine Zahl t_2 , welche für den Modul m_2 den Rest 1, für jeden der anderen Moduln den Rest Null giebt; weiter eine Zahl t_3 , welche $\equiv 1 \pmod{m_3}$, aber für jeden der anderen Moduln $\equiv 0$ ist; u. s. w.; endlich eine Zahl t_n , welche für den Modul m_n den Rest 1, für jeden der anderen Moduln den Rest Null giebt. Dann erfüllt offenbar die Zahl

$$x = r_1 t_1 + r_2 t_2 + \dots + r_n t_n$$

alle gestellten Bedingungen.

Beispiel. Es soll wieder

$$x \equiv 10 \pmod{67}, \quad \equiv 13 \pmod{15}, \quad \equiv 5 \pmod{7}$$

sein. Wir bestimmen zunächst t_1 durch die Kongruenzen

$$t_1 \equiv 1 \pmod{67}, \quad t_1 \equiv 0 \pmod{15}, \quad t_1 \equiv 0 \pmod{7}.$$

Wegen der beiden letzten Kongruenzen muß t_1 durch 15.7 teilbar, also von der Form $105t'_1$ sein, und aus

$$105t'_1 \equiv 1 \pmod{67}$$

folgt leicht

$$t'_1 \equiv 30 \pmod{67};$$

also ist

$$t'_1 = 30 + 67k \quad \text{und} \quad t_1 = 3150 + 7035k.$$

Ebenso bestimmen wir weiter t_2 durch die Kongruenzen

$$t_2 \equiv 0 \pmod{67}, \quad t_2 \equiv 1 \pmod{15}, \quad t_2 \equiv 0 \pmod{7}.$$

Die erste und dritte Kongruenz lehren, daß t_2 von der Form $469t'_2$ sein muß, und dann liefert die Kongruenz

$$469t'_2 \equiv 1 \pmod{15}$$

den Wert

$$t'_2 \equiv 4 \pmod{15}.$$

Es ist also

$$t'_2 = 4 + 15k \quad \text{und} \quad t_2 = 1876 + 7035k.$$

Endlich bestimmen wir t_3 durch die Kongruenzen

$$t_3 \equiv 0 \pmod{67}, \quad t_3 \equiv 0 \pmod{15}, \quad t_3 \equiv 1 \pmod{7}.$$

Mit Rücksicht auf die beiden ersten Kongruenzen ersetzen wir t_3 durch $1005t'_3$; dann geht die dritte Kongruenz über in $1005t'_3 \equiv 1 \pmod{7}$ und liefert $t'_3 \equiv 2 \pmod{7}$, so daß sich

$$t'_3 = 2 + 7k \quad \text{und} \quad t_3 = 2010 + 7035k$$

ergiebt. Als Wert von x erhalten wir also

$$10.3150 + 13.1876 + 5.2010 = 65938 \equiv 2623 \pmod{7035}.$$

Anmerkung. Die Anwendung der letzteren Methode setzt voraus, daß je zwei der Moduln $m_1, m_2, \dots$ prim zu einander seien. Wenn nämlich $m_1 = d\mu_1$ und $m_2 = d\mu_2$ einen größten gemeinschaftlichen Divisor d haben, so ist es unmöglich, den beiden Kongruenzen

$$t_1 \equiv 1 \pmod{d\mu_1}, \quad t_1 \equiv 0 \pmod{d\mu_2}$$

zu genügen; denn aus

$$t_1 = 1 + kd\mu_1 = ld\mu_2$$

folgt

$$d(l\mu_2 - k\mu_1) = 1,$$

und das ist unmöglich, da die linke Seite durch d teilbar ist, die rechte aber nicht. Auf diese Weise kann es kommen, daß die zweite Methode bei einer Aufgabe versagt, die recht wohl lösbar ist, und bei der die erste Methode zum Ziel führt.

Diesen Uebelstand zu beseitigen, zerlegen wir jeden der Moduln der gegebenen Kongruenzen in Zahlen, die entweder Primzahlen oder Potenzen von Primzahlen sind. Dann gilt die betreffende Kongruenz für jede dieser Zahlen als Modul. Wir gelangen so zu einer Reihe von Kongruenzen, von denen möglicherweise die eine oder die andere, weil mehrfach vorhanden, weggelassen werden kann. Es ist auch möglich, daß die eine Kongruenz einer anderen widerspricht; in diesem Falle ist die Aufgabe unmöglich. Wenn das nicht der Fall ist, bilden die neuen Kongruenzen ein System, in welchem je zwei Moduln prim zu einander sind, welches also der Anwendung der zweiten Methode unterliegt.

Beispiel. Welche Zahl giebt für die Divisoren 4, 6, 10 beziehungsweise die Reste 3, 5, 1?

Die erste Methode liefert für die gesuchte Zahl den Wert $x = 11 + 60k$, wo k jede ganze Zahl sein kann.

Nach der zweiten Methode haben wir es mit den Kongruenzen zu thun:

- 1) $x \equiv 3 \pmod{4}$;
- 2) $x \equiv 5 \pmod{6}$;
- 3) $x \equiv 1 \pmod{10}$.

Die zweite Kongruenz ersetzen wir durch

$$\begin{aligned} x &\equiv 5 \equiv 1 \pmod{2} \\ x &\equiv 5 \equiv -1 \pmod{3}, \end{aligned}$$

die dritte durch

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 1 \pmod{5}. \end{aligned}$$

Die Kongruenz $x \equiv 1 \pmod{2}$, die wir zweimal erhalten haben, kann überhaupt weggelassen werden, da sie in

$$x \equiv 3 \pmod{4}$$

enthalten ist. Wir haben somit die Kongruenzen

$$x \equiv 3 \pmod{4}, \quad x \equiv -1 \pmod{3}, \quad x \equiv 1 \pmod{5},$$

lasse man die Produkte $\alpha\xi$, $\beta\eta$, $\gamma\xi$, ... bilden und addieren. Die erhaltene Summe ist

$$\equiv x \pmod{abc\dots}.$$

Der kleinste positive Rest dieser Summe ist also die gedachte Zahl. Wieviele Zahlen a , b , c ... man wählt, ist gleichgültig.

Anmerkung. Die Aufgabe, die Zahl zu bestimmen, welche für gegebene Moduln gegebene Reste giebt, ist schon von den alten Chinesen gelöst worden (vergl. Biernatzki, Die Arithmetik der Chinesen. Crelles Journal, Bd. 52) und fehlt wohl in keinem arithmetischen Werke des Mittelalters. Die Aufgabe III ist die Nr. 5 der *Προβλήματα αριθμητικά* des Codex Cizensis¹⁾, welche Richard Hoche seiner Ausgabe der Arithmetik des Nikomachus beigelegt hat. Sie findet sich ebenfalls (für bestimmte Werte von a , b , c) bei vielen Schriftstellern des Mittelalters, z. B. bei Leonardo Pisano Bd. I, S. 304 der Ausgabe von Boncompagni.

§. 39.

Zerlegung eines Bruches in seine Partialbrüche.

Wir denken uns den Nenner N des vorgelegten Bruches in seine Primzahlfactoren zerlegt,

$$N = a^\alpha b^\beta \dots k^\kappa,$$

wo a , b , ..., k ungleiche Primzahlen, α , β , ..., κ ganze positive Zahlen bezeichnen. Wird nun der Kürze wegen

$$a^\alpha = A, \quad b^\beta = B, \quad c^\gamma = C, \dots, \quad k^\kappa = K$$

gesetzt, so ist jeder der Factoren des Produkts

$$N = ABC\dots K$$

prim zu jedem anderen. Den Bruch $\frac{Z}{N}$ in seine Partialbrüche zerlegen, heisst dann ihn auf die Form

$$\frac{Z}{N} = \frac{x}{A} + \frac{y}{B} + \frac{z}{C} + \dots + \frac{u}{K}$$

bringen, wo x , y , z , ..., u positive oder negative ganze Zahlen bedeuten.

¹⁾ Ciza = Zeitz.

Um diese Aufgabe zu lösen, multiplizieren wir beide Seiten der Gleichung mit N und erhalten

$$Z = BC \dots Kx + AC \dots Ky + AB \dots Kz + \dots + ABC \dots u.$$

Da nun alle Glieder der rechten Seite, mit Ausnahme des ersten, durch A teilbar sind; so erhalten wir zur Bestimmung von x die Kongruenz

$$BC \dots K.x \equiv Z \pmod{A}.$$

Ebenso ergeben sich weiter die Kongruenzen

$$AC \dots K.y \equiv Z \pmod{B},$$

$$AB \dots K.z \equiv Z \pmod{C},$$

$$\dots \dots \dots \dots \dots \dots$$

$$ABC \dots u \equiv Z \pmod{K},$$

welche beziehungsweise $y, z, \dots, u$ bestimmen.

Häufig empfiehlt es sich, nur positive echte Brüche im Endresultat zu dulden; das ermöglichen die beiden Formeln

$$-\frac{x}{A} = \frac{A-x}{A} - 1,$$

$$\frac{A+x}{A} = \frac{x}{A} + 1.$$

Beispiel. Es soll der Bruch $\frac{17}{60}$ in Partialbrüche zerlegt werden. Wird

$$\frac{17}{60} = \frac{x}{3} + \frac{y}{4} + \frac{z}{5}$$

gesetzt, so folgt durch Multiplikation mit 60

$$17 = 20x + 15y + 12z.$$

Es muß also

$20x \equiv 17 \pmod{3}$, $15y \equiv 17 \pmod{4}$, $12z \equiv 17 \pmod{5}$ sein, und diese Kongruenzen haben die Wurzeln

$$x \equiv 1 \pmod{3}, \quad y \equiv 3 \pmod{4}, \quad z \equiv 1 \pmod{5},$$

d. h. es ist

$$x = 1 + 3k, \quad y = 3 + 4k', \quad z = 1 + 5k'',$$

wo k, k', k'' unbestimmt bleiben. Für diese Werte wird

$$17 = 20(1 + 3k) + 15(3 + 4k') + 12(1 + 5k'')$$

oder

$$17 = 77 + 60(k + k' + k'').$$

Wir haben also über k, k', k'' so zu verfügen, daß

$$k + k' + k'' = -1$$

werde. Das ist auf unendlich viele Arten möglich. Will man jedoch als Partialbrüche nur echte Brüche zulassen, so ergeben sich für k, k', k'' nur die drei Wertsysteme

$$k = 0, \quad k' = 0, \quad k'' = -1,$$

$$k = 0, \quad k' = -1, \quad k'' = 0,$$

$$k = -1, \quad k' = 0, \quad k'' = 0,$$

denen die Lösungen

$$\frac{17}{60} = \frac{1}{3} + \frac{3}{4} - \frac{4}{5},$$

$$\frac{17}{60} = \frac{1}{3} - \frac{1}{4} + \frac{1}{5},$$

$$\frac{17}{60} = -\frac{2}{3} + \frac{3}{4} + \frac{1}{5}$$

entsprechen. Sollen die Brüche selbst positiv sein, so liefert die erste der angegebenen Formeln

$$\frac{17}{60} = \frac{1}{3} + \frac{3}{4} + \frac{1}{5} - 1.$$

Anmerkung. Der Bruch

$$\frac{Z}{a^\alpha b^\beta \dots k^\chi}$$

kann auch in Brüche mit den Nennern

$$a^\alpha, a^{\alpha-1}, \dots, a, b^\beta, b^{\beta-1}, \dots, b, \dots, k^\chi, k^{\chi-1}, \dots, k$$

zerlegt werden. Diese Zerlegung werden wir unten in §. 41 behandeln.

§. 40.

Auflösung der Gleichung

$$Ax + By + Cz + Du + \dots = \mu,$$

in welcher μ der größte gemeinschaftliche Divisor der Zahlen $A, B, C, D, \dots$ ist.

I. Wir behandeln zunächst die Gleichung

$$(1) \quad Ax + By = \mu_1,$$

wo μ_1 der grösste gemeinschaftliche Divisor von A und B ist. Dividieren wir beide Seiten durch μ_1 , so erhalten wir, wenn

$$\frac{A}{\mu_1} = a, \quad \frac{B}{\mu_1} = b$$

gesetzt wird, wo also a und b relative Primzahlen sein werden,

$$(2) \quad ax + by = 1.$$

Diese Gleichung ist der Kongruenz

$$ax \equiv 1 \pmod{b}$$

äquivalent, welche nach §. 34, Lehrsatz I eine einzige Wurzel $x \equiv \xi \pmod{b}$ hat. Es ist also $x = \xi + bk$, wo k unbestimmt bleibt, und durch Einsetzung dieses Wertes in (2) erhält man

$$y = \frac{1 - a\xi}{b} - ak$$

oder, wenn die ganze Zahl $\frac{1 - a\xi}{b}$ mit η bezeichnet wird, $y = \eta - ak$. Da k jede ganze Zahl sein kann, so hat die Gleichung (2) unendlich viele Lösungen.

Beispiel. Die Gleichung $5x - 8y = 1$ hat die Lösungen

$$x = +5 + 8k, \quad y = +3 + 5k,$$

wo k jede ganze Zahl sein kann.

II. Es sei jetzt die Gleichung

$$(3) \quad Ax + By + Cz = \mu_2$$

vorgelegt, wo μ_2 der grösste gemeinschaftliche Divisor der Zahlen A, B, C ist, der nach §. 16, Aufgabe II gefunden wird, indem man erst den grössten gemeinschaftlichen Divisor μ_1 von A und B , dann den grössten gemeinschaftlichen Divisor von μ_1 und C ermittelt. Ferner seien ξ, η die Wurzeln der Gleichung (1), also

$$A\xi + B\eta = \mu_1.$$

Auf dieselbe Weise wie (1) lösen wir die Gleichung

$$\mu_1 r + Cz = \mu_2,$$

deren Wurzeln $r = \varrho, z = \zeta$ sein mögen, so dafs also

$$\mu_1 \varrho + C\zeta = \mu_2$$

oder

$$(A\xi + B\eta)\varrho + C\zeta = \mu_2$$

oder

$$A.\xi\varrho + B.\eta\varrho + C\xi = \mu_2$$

ist, woraus hervorgeht, daß die Gleichung (3) die Wurzeln

$$x = \xi\varrho, \quad y = \eta\varrho, \quad z = \xi$$

hat.

III. Hat die linke Seite der vorgelegten Gleichung noch ein viertes Glied Du , so nehmen wir den größten gemeinschaftlichen Divisor μ_3 von μ_2 und D (der dann der größte gemeinschaftliche Divisor von A, B, C, D sein wird) und lösen nach I die Gleichung

$$\mu_2 s + Du = \mu_3,$$

deren Wurzeln $s = \sigma, u = v$ sein mögen, so daß also

$$\mu_2 \sigma + Dv = \mu_3$$

oder

$$(A\xi\varrho + B\eta\varrho + C\xi)\sigma + Dv = \mu_3$$

ist, was

$$x = \xi\varrho\sigma, \quad y = \eta\varrho\sigma, \quad z = \xi\sigma, \quad u = v$$

als Wurzeln der Gleichung

$$Ax + By + Cz + Du = \mu_3$$

ergiebt.

So fortfahrend gelangt man schließlich zur Lösung der Gleichung

$$Ax + By + Cz + Du + \dots = \mu,$$

in welcher μ den größten gemeinschaftlichen Divisor aller Zahlen $A, B, C, D, \dots$ bezeichnet.

Beispiel. Es soll eine Lösung der Gleichung

$$3x - 6y - 8z + 10u = 1$$

gefunden werden. Die Gleichung

$$3x - 6y = 3 \text{ hat die Wurzeln } x = 3, y = 1.$$

Weiter hat die Gleichung

$$3r - 8z = 1 \text{ die Wurzeln } r = 3, z = 1;$$

endlich hat die Gleichung

$$s + 10u = 1 \text{ die Wurzeln } s = 11, u = -1.$$

Es ist also

$x = 3 \cdot 3 \cdot 11 = 99$, $y = 1 \cdot 3 \cdot 11 = 33$, $z = 1 \cdot 11 = 11$, $u = -1$
eine Lösung der vorgelegten Gleichung.

Anmerkung. Wenn μ nicht der größte gemeinschaftliche Divisor der Koeffizienten $A, B, C, D, \dots$, sondern eine beliebige andere Zahl ist, so ist ein anderes Verfahren zur Lösung der Gleichung einzuschlagen, das in §. 41 dargelegt werden wird.

§. 41.

Auflösung der Kongruenz ersten Grades mit mehreren Unbekannten.

Die Kongruenz

$$ax + by + cz + \dots \equiv r \pmod{m}$$

oder die Gleichung

$$ax + by + cz + \dots = r + mk$$

ist offenbar nur dann möglich, wenn der größte gemeinschaftliche Divisor der Zahlen $a, b, c, \dots$ und m auch in r aufgeht. Wenn das der Fall ist, so fällt dieser Divisor durch Division weg; derselbe kann daher von vornherein gleich 1 angenommen werden.

Dies vorausgesetzt, lösen wir die Gleichung für die Unbekannte, welche den kleinsten Koeffizienten hat, wobei die übrigen Unbekannten zunächst als bekannt behandelt werden, und verfahren dann ganz auf die in §. 35 dargelegte Weise.

Aufgabe. (Bhāscara, Colebrooke, S. 233.) „5 Tauben sind für 3 Dramma zu haben, 7 Kraniche für 5, 9 Gänse für 7 und 3 Pfauen für 9 Dramma. Bringe 100 dieser Vögel für 100 Dramma zur Zufriedenheit des Fürsten.“

Es sind x Tauben, y Kraniche, z Gänse und $100 - x - y - z$ Pfauen, und die Preisangaben der Aufgabe liefern die Gleichung

$$\frac{3x}{5} + \frac{5y}{7} + \frac{7z}{9} + 3(100 - x - y - z) = 100,$$

welche nach leichten Reduktionen

$$189x + 180y + 175z = 15750$$

wird. Daraus folgt der Reihe nach

$$175z = 15750 - 180y - 189x,$$

$$z = 90 - y - x - \frac{5y + 14x}{175} = 90 - y - x - k,$$

$$5y = 175k - 14x,$$

$$y = 35k - 3x + \frac{x}{5} = 35k - 3x + k',$$

$$x = 5k',$$

so daß man

$$x = 5k',$$

$$y = 35k - 14k',$$

$$z = 90 - 36k + 9k',$$

$$100 - x - y - z = 10 + k$$

erhält, wo k und k' so zu wählen sind, daß sich für jede Unbekannte ein positiver Wert ergebe. Damit x positiv werde, ist k' positiv anzunehmen, und damit dann y positiv sei, muß auch k ein positiver Wert beigelegt werden. Aus den Ausdrücken für y und z erhält man

$$9y + 14z = -189k + 90.14,$$

und damit dieser Ausdruck positiv sei, muß $189k < 90.14$, also $k \leq 6$ sein. Für $k = 1$ kann k' (wegen y) nur die Werte 1, 2 haben. Wenn $k = 2$ ist, kann k' einen der vier Werte 1, 2, 3, 4 haben. Für $k = 3$ ist $z = 9k' - 18$, also muß k' wenigstens gleich 3 sein; es ist dann aber $y = 105 - 14k'$, also kann k' höchstens 7 sein, so daß sich für k' die fünf Werte 3, 4, 5, 6, 7 ergeben. Ebenso findet man für $k = 4$, daß k' die Werte 7, 8, 9 haben kann; für $k = 5$ kann $k' = 11$ oder 12 sein; die Annahme $k = 6$ endlich erweist sich als unmöglich. Wir erhalten also im ganzen 16 Lösungen, welche die folgende Tabelle darstellt.

k	k'	x	y	z	$100 - x - y - z$
1	1	5	21	63	11
	2	10	7	72	11
2	1	5	56	27	12
	2	10	42	36	12
	3	15	28	45	12
	4	20	14	54	12

k	k'	x	y	z	$100 - x - y - z$
3	3	15	63	9	13
	4	20	49	18	13
	5	25	35	27	13
	6	30	21	36	13
	7	35	7	45	13
4	7	5	42	9	14
	8	40	28	18	14
	9	45	14	27	14
5	11	55	21	9	15
	12	60	7	18	15

Zerlegung eines Bruches in Partialbrüche. Auf eine Gleichung mit mehreren Unbekannten wird auch die in der Anmerkung zu §. 39 erwähnte Aufgabe zurückgeführt, einen Bruch mit dem Nenner $a^\alpha b^\beta \dots k^\kappa$, wo $a, b, \dots, k$ ungleiche Primzahlen bezeichnen, in Brüche mit den Nennern

$$a^\alpha, a^{\alpha-1}, \dots, a, b^\beta, \dots, b, \dots, k$$

zu zerlegen. Aus der Gleichung

$$\frac{Z}{a^\alpha b^\beta \dots k^\kappa} = \frac{x_1}{a^\alpha} + \frac{x_2}{a^{\alpha-1}} + \dots + \frac{x_\alpha}{a} + \frac{y_1}{b^\beta} + \dots + \frac{y_\beta}{b} + \dots + \frac{z_\kappa}{k}$$

folgt nämlich durch Multiplikation mit $a^\alpha b^\beta \dots k^\kappa$

$$Z = b^\beta \dots k^\kappa x_1 + a b^\beta \dots k^\kappa x_2 + \dots + a^{\alpha-1} b^\beta \dots k^\kappa x_\alpha + a^\alpha b^\beta \dots k^\kappa y_1 + \dots,$$

und diese Gleichung ist in der oben dargelegten Weise zu behandeln.

Auch hier hat man besondere Sorgfalt anzuwenden, wenn man alle Lösungen finden will, die die Aufgabe zuläßt.

Beispiel. Es soll der Bruch $\frac{59}{72}$ zerlegt werden. Die Annahme

$$\frac{59}{72} = \frac{x_1}{8} + \frac{x_2}{4} + \frac{x_3}{2} + \frac{y_1}{9} + \frac{y_2}{3}$$

liefert

$$59 = 9x_1 + 18x_2 + 36x_3 + 8y_1 + 24y_2,$$

und daraus folgt

$$8y_1 = 59 - 9x_1 - 18x_2 - 36x_3 - 24y_2$$

oder

$$y_1 = 7 - x_1 - 2x_2 - 4x_3 - 3y_2 + \frac{3 - x_1 - 2x_2 - 4x_3}{8}.$$

Wird jetzt

$$\frac{3 - x_1 - 2x_2 - 4x_3}{8} = k$$

gesetzt, so erhält man

$$\begin{cases} x_1 = 3 - 2x_2 - 4x_3 - 8k \\ y_1 = 4 - 3y_2 + 9k, \end{cases}$$

wo x_1, x_2, y_2, k noch unbestimmt sind.

Da es sich hier nur um echte Brüche handelt, so kann x_3 nur die beiden Werte ± 1 haben, y_2 nur die vier Werte $\pm 1, \pm 2$, und ebenso giebt es Grenzen für x_1, x_2, y_1 .

Wenn nun erstens $x_3 = +1$ ist, so erkennt man leicht, daß k entweder $= 0$ oder $= +1$ oder $= -1$ sein muß. Für $k = 0$ kann y_2 jeder der drei Werte $+1, -1, +2$ und x_2 jeder der sechs Werte $\pm 1, \pm 2, \pm 3$ beigelegt werden. Da somit 18 Verbindungen je eines Wertes von y_2 mit einem Werte von x_2 möglich sind, so liefert dieser Fall 18 Lösungen. Für $k = +1$ kann y_2 nur $+2$ sein, während x_2 jeden der drei Werte $-1, -2, -3$ haben kann; wir erhalten auf diese Weise drei weitere Lösungen. Für $k = -1$ endlich sind für y_2 die drei Werte $\pm 1, -2$, für x_2 die drei Werte $+1, +2, +3$ zulässig, so daß sich neun Lösungen ergeben.

Wenn zweitens $x_3 = -1$ ist, so kann $k = 0$ oder $= +1$ sein. Für $k = 0$ kann y_2 jeden der drei Werte $\pm 1, +2$ und x_2 jeden der drei Werte $+1, +2, +3$ erhalten; das ergiebt neun Lösungen. Für $k = +1$ sind für x_2 die sechs Werte $\pm 1, \pm 2, \pm 3$, für y_2 nur der eine Wert $+2$ möglich, was sechs Lösungen liefert. Die Aufgabe läßt also im ganzen $18 + 3 + 9 + 9 + 6 = 45$ Lösungen zu.

§. 42.

Auflösung eines Systems von m Kongruenzen ersten Grades mit m oder mehr Unbekannten.

1. Fall. Die Kongruenzen gelten für denselben Modul. Man bildet durch Elimination entweder ein zweites System, in

welchem jede folgende Kongruenz eine Unbekannte weniger als die vorhergehende enthält; oder man leitet aus dem vorgelegten System ein zweites her, welches eine Kongruenz und eine Unbekannte weniger als das erste enthält, aus diesem ein drittes, welches eine Kongruenz und eine Unbekannte weniger als das zweite enthält, und fährt so fort, bis man zu einem System gelangt, das nur aus einer Kongruenz besteht. Die Werte der Unbekannten, welche die Auflösung der letzten Kongruenz des zweiten Systems, resp. der Kongruenz des letzten Systems liefert, werden in die übrigen Kongruenzen eingesetzt und dadurch die Werte der übrigen Unbekannten der Reihe nach bestimmt.

Beispiel. Es sei das System

$$\left. \begin{array}{l} 3x - 4y + 5z - 9u \equiv 1 \\ 2x + 3y + 4z + 5u \equiv 8 \\ x + 5y + 6z + 2u \equiv 1 \end{array} \right\} \text{(mod. 15)}$$

gegeben. Wir setzen den aus der dritten Kongruenz genommenen Wert

$$x \equiv 1 - 5y - 6z - 2u \text{ (mod. 15)}$$

in die beiden ersten ein und erhalten

$$\left. \begin{array}{l} -7y - 8z + u \equiv 6 \\ -2y + z \equiv -1 \end{array} \right\} \text{(mod. 15)}.$$

Die zweite dieser Kongruenzen liefert

$$z \equiv 2y - 1 \text{ (mod. 15),}$$

und dieser Wert verwandelt die erste in

$$-8y + u \equiv -2 \text{ (mod. 15)}.$$

Das neue System ist also

$$\left. \begin{array}{l} x \equiv 1 - 5y - 6z - 2u \\ z \equiv 2y - 1 \\ -8y + u \equiv -2 \end{array} \right\} \text{(mod. 15)}.$$

y bleibt unbestimmt; die letzte Kongruenz liefert u , die vorletzte z , die erste x . Man erhält

$$u \equiv 8y - 2, \quad z \equiv 2y - 1, \quad x \equiv 11 - 3y \text{ (mod. 15)}.$$

Man hätte auch aus dem vorgelegten System durch Elimination von x

$$\left. \begin{array}{l} 2y - z \equiv 1 \\ 7y + 8z - u \equiv -6 \end{array} \right\} \text{(mod. 15)}$$

und hieraus durch Elimination von z

$$8y - u \equiv 2 \pmod{15}$$

herleiten und dann die Lösung, wie oben dargelegt ist, beenden können.

2. Fall. Die Kongruenzen beziehen sich auf verschiedene Moduln. Man ersetzt jede Kongruenz durch die entsprechende unbestimmte Gleichung. Diese Gleichungen können auch direkt durch die Aufgabe gegeben sein. Man bildet aus ihnen durch Elimination eine Gleichung, welche $m - 1$ der Unbekannten nicht mehr enthält, und wendet auf sie das Verfahren des §. 35 an.

Beispiel. (Euler, Algebra Bd. II, §. 30.) Drei ganze positive Zahlen x, y, z zu finden, welche den Gleichungen

$$3x + 5y + 7z = 560$$

$$9x + 25y + 49z = 2920$$

genügen. Durch Elimination von x erhält man

$$5y + 14z = 620.$$

Es ist also

$$14z \equiv 620 \pmod{5},$$

und daraus folgt

$$z \equiv 0 \pmod{5} \quad \text{oder} \quad z = 5k.$$

Für diesen Wert wird

$$5y + 70k = 620,$$

also

$$y = 124 - 14k,$$

und die erste Gleichung geht über in

$$3x + 620 - 70k + 35k = 560,$$

woraus

$$3x = -60 + 35k$$

folgt. k muß danach durch 3 teilbar sein. Wir setzen $k = 3l$ und erhalten schliesslich

$$x = -20 + 35l, \quad y = 124 - 42l, \quad z = 15l,$$

wo l jede ganze Zahl sein kann, welche für x, y, z positive Werte liefert. Es ergeben sich die beiden Lösungen

$$x = 15, \quad y = 82, \quad z = 15;$$

$$x = 50, \quad y = 40, \quad z = 30.$$

§. 43.

Der Wilsonsche Satz.

Das um 1 vermehrte Produkt aller Zahlen von 1 bis $p - 1$, also die Zahl

$$Z = 1.2.3... (p - 1) + 1$$

ist durch p teilbar, wenn p eine Primzahl ist, sonst nicht.

I. Beweis (Lagrange, Nouveaux Mémoires de l'Acad. de Berlin 1771 = Oeuvres III, p. 425).

Wir setzen

(1) $(x+1)(x+2)...(x+n-1) = x^{n-1} + A_1 x^{n-2} + \dots + A_{n-1}$;
 darin bezeichnet, wie leicht ersichtlich, A_1 die Summe der Zahlen 1, 2, ..., $n - 1$; weiter ist A_2 die Summe aller durch Multiplikation je zweier dieser Zahlen erhaltenen Produkte, u. s. w.; A_{n-1} endlich ist das Produkt $1.2.3...(n-1)$. Die Koeffizienten $A_1, A_2, \dots, A_{n-1}$ sind also ganze Zahlen.

Wird in (1) x durch $x + 1$ ersetzt, so folgt

$$(2) (x+2)(x+3)...(x+n) = (x+1)^{n-1} + A_1 (x+1)^{n-2} + \dots + A_{n-1}$$

oder, wenn beiderseits mit $x + 1$ multipliziert wird,

$$(3) (x+1)(x+2)...(x+n) = (x+1)^n + A_1 (x+1)^{n-1} + \dots + A_{n-1} (x+1).$$

Andererseits ergibt sich, wenn man (1) mit $x + n$ multipliziert,

$$(4) (x+1)(x+2)...(x+n) = x^n + (n+A_1)x^{n-1} + (nA_1+A_2)x^{n-2} + (nA_2+A_3)x^{n-3} + \dots + (nA_{n-2}+A_{n-1})x + nA_{n-1}.$$

Wenn man jetzt die Potenzen von $(x + 1)$ in (3) entwickelt und die Koeffizienten der gleichen Potenzen von x in (3) und (4) einander gleich setzt, so erhält man

$$\begin{aligned} n + A_1 &= n + A_1 \\ nA_1 + A_2 &= \frac{n(n-1)}{2} + (n-1)A_1 + A_2 \\ nA_2 + A_3 &= \frac{n(n-1)(n-2)}{1.2.3} + \frac{(n-1)(n-2)}{1.2}A_1 + (n-2)A_2 + A_3 \\ &\dots \end{aligned}$$

und daraus ergibt sich

$$(5) \quad \left\{ \begin{array}{l} A_1 = \frac{n(n-1)}{2} \\ 2 A_2 = \frac{n(n-1)(n-2)}{1.2.3} + \frac{(n-1)(n-2)}{1.2} A_1 \\ 3 A_3 = \frac{n(n-1)(n-2)(n-3)}{1.2.3.4} + \frac{(n-1)(n-2)(n-3)}{1.2.3} A_1 \\ \quad + \frac{(n-2)(n-3)}{1.2} A_2 \\ \dots \end{array} \right.$$

Wenn n eine ganze Zahl ist, so sind bekanntlich auch die Ausdrücke

$$\frac{n(n-1)}{1.2}, \frac{n(n-1)(n-2)}{1.2.3}, \dots; \frac{(n-1)(n-2)}{1.2},$$

$$\frac{(n-1)(n-2)(n-3)}{1.2.3}, \dots; \frac{(n-2)(n-3)}{1.2}, \dots$$

ganze Zahlen. Wir nehmen jetzt an, n sei eine Primzahl; dann ist jede der Zahlen

$$\frac{n(n-1)}{1.2}, \frac{n(n-1)(n-2)}{1.2.3}, \dots$$

bis auf die letzte, d. i.

$$\frac{n(n-1) \dots 1}{1.2 \dots n},$$

welche den Wert 1 hat, durch n teilbar, denn jede enthält den Faktor n im Zähler, im Nenner aber nur Faktoren, die kleiner als n sind, so daß die Primzahl n sich nicht wegheben kann. Unter dieser Voraussetzung lehrt dann die erste der Formeln (5), daß A_1 durch n teilbar ist; dann lassen die übrigen Formeln (5) erkennen, daß $2 A_2, 3 A_3, \dots, (n-2) A_{n-2}$ durch n teilbar sind; es müssen also auch die Zahlen

$$A_1, A_2, \dots, A_{n-2}$$

selbst durch n teilbar sein (§. 17, Satz 1).

Was nun A_{n-1} betrifft, so wird diese Zahl durch die Formel

$$(n-1) A_{n-1} = \frac{n(n-1) \dots 1}{1.2 \dots n} + \frac{(n-1)(n-2) \dots 1}{1.2 \dots (n-1)} A_1$$

$$+ \frac{(n-2)(n-3) \dots 1}{1.2.3 \dots (n-2)} A_2 + \dots,$$

d. i. durch

$$(n-1)A_{n-1} = 1 + A_1 + A_2 + \dots + A_{n-2}$$

bestimmt, und da

$$n \equiv 0, \quad A_1 \equiv 0, \quad A_2 \equiv 0, \dots, \quad A_{n-2} \equiv 0 \pmod{n}$$

ist, so erhalten wir $-A_{n-1} \equiv 1 \pmod{n}$ oder

$$A_{n-1} + 1, \text{ d. i. } 1.2.3\dots(n-1) + 1 \equiv 0 \pmod{n}.$$

Für jede Primzahl p ist also die Zahl

$$1.2.3\dots(p-1) + 1$$

durch p teilbar.

Ist dagegen n keine Primzahl, sondern durch eine Primzahl $q < n$ teilbar, so tritt q als Faktor in dem Produkt $1.2\dots(n-1)$ auf. Die Zahl $1.2.3\dots(n-1) + 1$ ist also nicht durch q und somit auch nicht durch n teilbar.

II. Beweis (Gauss, Disquisitiones, 77). Es sei p eine Primzahl und a irgend eine der Zahlen $1, 2, 3, \dots, p-1$. Da dann a prim zu p ist, so hat die Kongruenz

$$ax \equiv 1 \pmod{p}$$

nach §. 34, Lehrsatz II stets eine, aber auch nur eine Wurzel. Wäre diese Wurzel gleich dem Koeffizienten a , also $a^2 \equiv 1 \pmod{p}$, so müßte $a^2 - 1$, also entweder $a + 1$ oder $a - 1$ durch p teilbar sein. Nun ist aber $a < p$. Ginge also p in $a + 1$ auf, so müßte $a + 1 = p$, also $a = p - 1$ sein, und ginge p in $a - 1$ auf, so müßte $a - 1 = 0$, also $a = 1$ sein. Wenn daher a weder 1, noch $p - 1$ ist, sondern eine der Zahlen $2, 3, \dots, p-2$, so kann die Wurzel der Kongruenz $ax \equiv 1 \pmod{p}$ nie gleich dem Koeffizienten a sein. Ferner können zwei Kongruenzen mit ungleichen Koeffizienten a, a'

$$ax \equiv 1, \quad a'x \equiv 1 \pmod{p}$$

nicht dieselbe Wurzel x haben; denn sonst würde die Kongruenz

$$ax \equiv a'x \pmod{p}$$

durch Division mit x in $a \equiv a' \pmod{p}$ übergehen, während zwei verschiedene Zahlen der Reihe $2, 3, \dots, p-2$ für den Modul p nicht kongruent sein können. Die Zahlen $2, 3, \dots, p-2$ lassen sich somit in Gruppen von je zweien in der Weise zusammenstellen, daß das Produkt der Zahlen jeder Gruppe den

Rest 1 liefert. Durch Multiplikation aller so gebildeten Kongruenzen erhält man

$$2 \cdot 3 \cdot 4 \dots (p-2) \equiv 1 \pmod{p},$$

und hieraus folgt durch Multiplikation mit $1 \cdot (p-1)$

$$1 \cdot 2 \cdot 3 \dots (p-2)(p-1) \equiv p-1 \equiv -1 \pmod{p},$$

d. h. es ist unter der gemachten Voraussetzung

$$1 \cdot 2 \cdot 3 \dots (p-1) + 1$$

durch p teilbar.

III. Beweis (Stern, Algebraische Analysis, S. 391). Für $x < 1$ ist bekanntlich

$$\log(1-x) = -x - \frac{x^2}{2} - \frac{x^3}{3} - \dots,$$

also

$$-\log(1-x) = \log \frac{1}{1-x} = x + \frac{x^2}{2} + \frac{x^3}{3} + \dots,$$

und mithin

$$e^{x + \frac{x^2}{2} + \frac{x^3}{3} + \dots} = \frac{1}{1-x} = 1 + x + x^2 + x^3 + \dots,$$

oder

$$e^x \cdot e^{\frac{x^2}{2}} \cdot e^{\frac{x^3}{3}} \dots = 1 + x + x^2 + x^3 + \dots,$$

d. h.

$$\begin{aligned} & \left(1 + \frac{x}{1} + \frac{x^2}{1 \cdot 2} + \frac{x^3}{1 \cdot 2 \cdot 3} + \dots\right) \left(1 + \frac{\frac{1}{2}x^2}{1} + \frac{\frac{1}{4}x^4}{1 \cdot 2} + \dots\right) \\ & \quad \left(1 + \frac{\frac{1}{3}x^3}{1} + \frac{\frac{1}{9}x^6}{1 \cdot 2} + \dots\right) \dots \\ & = 1 + x + x^2 + x^3 + \dots \end{aligned}$$

Wir denken uns jetzt das Produkt der linken Seite entwickelt und setzen, unter p eine Primzahl verstehend, die beiderseitigen Glieder mit x^p einander gleich. Es ergibt sich

$$\begin{aligned} & \frac{x^p}{1 \cdot 2 \cdot 3 \dots p} + \frac{x^{p-2}}{1 \cdot 2 \dots (p-2)} \cdot \frac{1}{2}x^2 + \frac{x^{p-4}}{1 \cdot 2 \dots (p-4)} \cdot \frac{1}{1 \cdot 2}x^4 + \dots \\ & + \frac{x^{p-3}}{1 \cdot 2 \dots (p-3)} \cdot \frac{1}{3}x^3 + \dots + \frac{1}{p}x^p + \dots = x^p. \end{aligned}$$

Von allen Gliedern der linken Seite haben nur

$$\frac{x^p}{1 \cdot 2 \cdot 3 \dots p} \quad \text{und} \quad \frac{x^p}{p}$$

die Primzahl p im Nenner. Wird die Summe der übrigen Glieder mit $s.x^p$ bezeichnet, so ist s , auf seine kleinste Benennung gebracht, ein Bruch, welcher nicht den Faktor p im Nenner hat. Es ergibt sich dann durch Division mit x^p

$$\frac{1}{1.2.3\dots p} + s + \frac{1}{p} = 1$$

oder

$$1 - s = \frac{1}{1.2.3\dots p} + \frac{1}{p}.$$

Hieraus folgt

$$(1 - s).1.2.3\dots(p-1) = \frac{1 + 1.2.3\dots(p-1)}{p},$$

und da die linke Seite kein Bruch mit dem Nenner p sein kann, so muß $1.2.3\dots(p-1) + 1$ durch p teilbar sein.

Anmerkung. E. Waring, der den Satz zuerst, allerdings ohne Beweis, gebracht hat (*Meditationes algebraicae*, 1770, p. 218) schreibt ihn dem Johann Wilson zu. Der Satz liefert eine untrügliche, aber wegen der ungeheuren Rechnung, die sie erfordert, in der Praxis gar nicht anzuwendende Regel, zu erkennen, ob eine gegebene Zahl eine Primzahl oder zusammengesetzt sei. Unten in §. 45, 47 und 83 werden wir noch andere Beweise geben, und eine Verallgemeinerung des Satzes wird in §. 113 hergeleitet werden.

Zusatz. Je nachdem p eine Primzahl von der Form $4n + 1$ oder $4n + 3$ ist, ist

$$\left[1.2.3\dots\frac{p-1}{2}\right]^2 + 1 \quad \text{oder} \quad \left[1.2.3\dots\frac{p-1}{2}\right]^2 - 1$$

durch p teilbar (Lagrange, l. c.).

Beweis. Wenn man in der Reihe

$$(1) \quad 1, 2, 3, \dots, \frac{p-1}{2}, \frac{p+1}{2}, \dots, (p-1)$$

jede Zahl, die $> \frac{p}{2}$ ist, durch ihren absolut kleinsten Rest für den Modul p ersetzt, so erhält man die Reihe

$$(2) \quad 1, 2, 3, \dots, \frac{p-1}{2}, -\frac{p-1}{2}, -\frac{p-3}{2}, \dots, -3, -2, -1,$$

und das Produkt dieser letzteren Zahlen ist dem Produkt

$$1 \cdot 2 \cdot 3 \dots (p-1)$$

für den Modul p kongruent. Die Reihe (2) enthält aber $\frac{p-1}{2}$ negative Glieder, und $\frac{p-1}{2}$ ist gerade oder ungerade, je nachdem p von der Form $4n+1$ oder $4n+3$ ist. Im ersteren Falle ist also

$$1 \cdot 2 \cdot 3 \dots (p-1) \equiv + \left[1 \cdot 2 \dots \frac{p-1}{2} \right]^2,$$

im zweiten ist

$$1 \cdot 2 \cdot 3 \dots (p-1) \equiv - \left[1 \cdot 2 \dots \frac{p-1}{2} \right]^2 \pmod{p},$$

und somit lehrt der Wilsonsche Satz, daß im ersten Falle

$$\left[1 \cdot 2 \cdot 3 \dots \frac{p-1}{2} \right]^2 + 1,$$

im zweiten

$$- \left[1 \cdot 2 \cdot 3 \dots \frac{p-1}{2} \right]^2 + 1,$$

also auch

$$\left[1 \cdot 2 \cdot 3 \dots \frac{p-1}{2} \right]^2 - 1$$

durch p teilbar ist.

Aufgabe. Leite aus dem Wilsonschen Satze die Formeln

$$\left. \begin{array}{l} 1 \cdot 2 \cdot 3 \dots (p-2) - 1 \equiv 0 \\ 1 \cdot 2^2 \cdot 3 \dots (p-3) + 1 \equiv 0 \\ 1 \cdot 2^3 \cdot 3^2 \cdot 4 \dots (p-4) - 1 \equiv 0 \\ \dots \dots \dots \end{array} \right\} \pmod{p}$$

her.

§. 44.

Der Fermatsche Satz.

Bezeichnet a eine beliebige durch die Primzahl p nicht teilbare ganze Zahl, so ist

$$a^{p-1} \equiv 1 \pmod{p},$$

oder mit anderen Worten: Die Kongruenz

$$x^{p-1} \equiv 1 \pmod{p}$$

hat jede der $p-1$ Zahlen $1, 2, 3, \dots, p-1$ zur Wurzel.

I. Beweis (Euler, *Commentationes arithmeticae collectae* I, p. 21 ff.). Bezeichnet p eine Primzahl, so sind die Koeffizienten

$$\frac{p}{1}, \quad \frac{p(p-1)}{1 \cdot 2}, \quad \frac{p(p-1)(p-2)}{1 \cdot 2 \cdot 3}, \quad \dots, \quad \frac{p}{1}$$

in der Entwicklung

$$(a+1)^p = a^p + \frac{p}{1} a^{p-1} + \frac{p(p-1)}{1 \cdot 2} a^{p-2} + \dots + \frac{p}{1} a + 1,$$

da in keinem Nenner die Primzahl p vorkommt, sämtlich durch p teilbar, also

$$(a+1)^p \equiv a^p + 1 \pmod{p}$$

oder

$$(a+1)^p - (a+1) \equiv a^p - a \pmod{p}.$$

Wenn also $a^p - a$ durch p teilbar ist, so ist es auch $(a+1)^p - (a+1)$. Nun ist aber $1^p - 1 \equiv 0 \pmod{p}$; folglich ist auch $2^p - 2$, weiter $3^p - 3$, u. s. w. durch p teilbar. Wenn aber $a^p - a = a(a^{p-1} - 1)$ durch p teilbar und a durch die Primzahl p nicht teilbar ist, so muß $a^{p-1} - 1$ durch p teilbar, d. h.

$$a^{p-1} \equiv 1 \pmod{p}$$

sein.

II. Beweis (J. H. Lambert, *Nova Acta Eruditorum*, 1769). Es sei a eine beliebige durch die Primzahl p nicht teilbare ganze Zahl, und es werde $a = b + 1$ gesetzt. Dann ist

$$\begin{aligned} a^{p-1} - 1 &= (b+1)^{p-1} - 1 \\ &= -1 + b^{p-1} + (p-1)b^{p-2} + \frac{(p-1)(p-2)}{1 \cdot 2} b^{p-3} + \dots + 1 \end{aligned}$$

oder, wenn die Gesamtheit der durch p teilbaren Glieder der rechten Seite mit pA bezeichnet wird,

$$a^{p-1} - 1 = -1 + pA + [b^{p-1} - b^{p-2} + b^{p-3} - \dots + 1].$$

Wird die geometrische Reihe der rechten Seite durch ihre Summe ersetzt, so geht diese Formel über in

$$a^{p-1} - 1 = -1 + pA + \frac{b^p + 1}{b + 1}$$

oder, was dasselbe ist, in

$$\begin{aligned} a^{p-1} - 1 &= -1 + pA + b^{p-1} - \frac{b^{p-1} - 1}{b + 1} \\ &= pA + (b^{p-1} - 1) - \frac{b^{p-1} - 1}{b + 1}. \end{aligned}$$

Durch Division mit p folgt hieraus

$$\frac{a^{p-1} - 1}{p} = A + \frac{b^{p-1} - 1}{p} - \frac{b^{p-1} - 1}{p(b+1)}.$$

Nun ist

$$\frac{b^{p-1} - 1}{b+1} = \frac{(a-1)^{p-1} - 1}{a}$$

eine ganze Zahl, und da p prim zu a ist, so wird

$$\frac{b^{p-1} - 1}{p(b+1)}$$

eine ganze Zahl sein, wenn p in $b^{p-1} - 1$ aufgeht, und unter dieser Bedingung ist dann auch

$$\frac{a^{p-1} - 1}{p}$$

eine ganze Zahl.

Der Fermatsche Satz ist also für $a = b + 1$ richtig, wenn er für b richtig ist. Da er nun für die Zahl 1 besteht, so gilt er auch für 2, weiter für 3, u. s. w., also allgemein für jede durch p nicht teilbare Zahl a .

III. Beweis (Lagrange, Nouveaux Mémoires de l'Acad. de Berlin, 1771 = Oeuvres III, p. 425).

In seinem Beweis des Wilsonschen Satzes setzt Lagrange $(x+1)(x+2)\dots(x+p-1) = x^{p-1} + A_1 x^{p-2} + \dots + A_{p-1}$ und beweist, daß jede der Zahlen $A_1, A_2, \dots, A_{p-2}$ durch die Primzahl p teilbar, daß also

$$(x+1)(x+2)\dots(x+p-1) \equiv x^{p-1} + A_{p-1} \pmod{p}$$

ist.

Wenn nun x weder gleich Null, noch durch p teilbar ist, so ist jedenfalls ein Faktor des Produkts $(x+1)\dots(x+p-1)$ durch p teilbar, also

$$x^{p-1} + A_{p-1} \equiv 0 \pmod{p},$$

und da, wie wir in §. 43 bewiesen haben,

$$A_{p-1} \equiv -1 \pmod{p}$$

ist, so ergibt sich

$$x^{p-1} - 1 \equiv 0 \pmod{p}.$$

IV. Beweis (Laplace in Lacroix, *Traité du calcul différentiel et intégral*, T. III, p. 722). Es ist

$$\begin{aligned} a^{p-1} &= \frac{a^p}{a} = \frac{1}{a} [(a-1) + 1]^p \\ &= \frac{1}{a} \left[(a-1)^p + \frac{p}{1} (a-1)^{p-1} + \frac{p(p-1)}{1 \cdot 2} (a-1)^{p-2} + \dots \right. \\ &\quad \left. + \frac{p}{1} (a-1) + 1 \right]. \end{aligned}$$

Wird hierin p als Primzahl vorausgesetzt, so sind die Koeffizienten der Potenzen

$$(a-1)^{p-1}, (a-1)^{p-2}, \dots, (a-1)$$

sämtlich durch p teilbar. Wir können also

$$a^{p-1} = \frac{1}{a} [(a-1)^p + Ep(a-1) + 1]$$

schreiben, wo E eine ganze Zahl bezeichnet. Daraus folgt

$$\begin{aligned} a^{p-1} - 1 &= \frac{1}{a} [(a-1)^p + Ep(a-1) + 1] - 1 \\ &= \frac{1}{a} [(a-1)^p + Ep(a-1) + 1 - a] \\ &= \frac{a-1}{a} [(a-1)^{p-1} + Ep - 1]. \end{aligned}$$

Wenn nun zunächst $a < p$ ist, so lehrt die letzte Formel, daß $a^{p-1} - 1$ durch p teilbar ist, wenn p in $(a-1)^{p-1} - 1$ aufgeht, und da $1^{p-1} - 1 \equiv 0 \pmod{p}$ ist, so folgt hieraus wie oben die Richtigkeit des Satzes für jede Zahl $a < p$.

Ist weiter $a > p$, etwa $a = np + q$, wo $q < p$ sein möge, so ergibt sich $a^{p-1} - 1$, d. i. $-1 + (q + np)^{p-1}$

$$= -1 + q^{p-1} + \frac{p-1}{1} q^{p-2} np + \dots + n^{p-1} p^{p-1},$$

und da alle Glieder der rechten Seite, mit Ausnahme der beiden ersten, den Faktor p enthalten, so ist

$$a^{p-1} - 1 \equiv -1 + q^{p-1} \pmod{p}.$$

Da aber $q < p$ ist, so ist die rechte Seite dieser Kongruenz durch p teilbar, folglich ist auch

$$a^{p-1} - 1 \equiv 0 \pmod{p}.$$

V. Beweis [Gauss¹⁾, Disquisitiones, 51]. Wenn man die Potenz $(a + b + c + \dots)^p$ nach dem polynomischen Satz entwickelt, so erhält man auſſer den p^{ten} Potenzen der Zahlen $a, b, c, \dots$ eine Reihe Glieder von der Form $ka^{\alpha}b^{\beta}c^{\gamma} \dots$, wo $\alpha + \beta + \gamma + \dots = p$ und

$$k = \frac{1 \cdot 2 \cdot 3 \dots p}{1 \cdot 2 \dots \alpha \cdot 1 \cdot 2 \dots \beta \cdot 1 \cdot 2 \dots \gamma \dots},$$

also eine durch p teilbare ganze Zahl ist. Es ist somit

$$(a + b + c + \dots)^p \equiv a^p + b^p + c^p + \dots \pmod{p}.$$

Wird jetzt jede der m Zahlen $a, b, c, \dots$ gleich 1 vorausgesetzt, so geht diese Kongruenz über in

$$m^p \equiv m \pmod{p},$$

und hieraus folgt, wenn m durch p nicht teilbar ist,

$$m^{p-1} \equiv 1 \pmod{p}.$$

VI. Beweis (Lejeune Dirichlet, Crelles Journal III, S. 392 = Werke I, S. 103). Wir betrachten die Produkte, die man erhält, wenn man jede der Zahlen

$$(1) \quad 1, 2, 3, \dots, p-1$$

mit a multipliziert, also die Zahlen

$$(2) \quad a, 2a, 3a, \dots, (p-1)a.$$

Die Reste dieser Produkte für den Modul p müssen sämtlich von einander verschieden sein; denn aus der Annahme

$$ka \equiv k'a \pmod{p}$$

würde sich durch Division mit a

$$k \equiv k' \pmod{p}$$

ergeben, während zwei verschiedene Zahlen der Reihe (1), und als solche werden k und k' vorausgesetzt, nicht kongruent sein können. Da auſſerdem keins der Produkte (2) durch p teilbar ist, so müssen die Reste der Zahlen (2) in irgend einer Reihen-

¹⁾ In der Bibliotheca mathematica 1894 macht G. Vacca darauf aufmerksam, daß Leibniz einen ganz ähnlichen Beweis gefunden hat, der in Bd. VII, S. 180 seiner Math. Schriften (herausgegeben von J. C. Gerhardt) veröffentlicht ist. Leibniz (nicht Euler) hat also den ersten Beweis des Fermatschen Satzes gegeben.

folge mit den Zahlen (1) übereinstimmen, und es muß folglich das Produkt aller Zahlen (2) dem Produkt aller Zahlen (1) kongruent sein, d. h. es ist

$$1.2.3...(p-1)a^{p-1} \equiv 1.2.3...(p-1) \pmod{p}.$$

Hieraus ergibt sich durch Division mit $1.2.3...(p-1)$

$$a^{p-1} \equiv 1 \pmod{p}.$$

Anmerkung. Der Satz ist von seinem Entdecker Pierre de Fermat ohne Beweis in einem Briefe an Frenicle (18. Oktober 1640) mitgeteilt worden (*Varia opera mathematica*, p. 163 = *Oeuvres* Bd. II, S. 209). Unten in §. 72 werden wir noch einen anderen von Euler gegebenen Beweis mitteilen, und Eulers Verallgemeinerung des Satzes wird in §. 88 behandelt werden.

§. 45.

Anwendungen des Fermatschen Satzes.

I. Lagranges zweiter Beweis des Wilsonschen Satzes (*Nouveaux Mémoires de l'Acad. de Berlin* 1771 = *Oeuvres* III, p. 433). Wir betrachten die Reihe

$$(1) \quad 1^{n-1}, 2^{n-1}, 3^{n-1}, \dots, (n-1)^{n-1}, n^{n-1}.$$

Die ersten Differenzen derselben sind

$$2^{n-1} - 1^{n-1}, 3^{n-1} - 2^{n-1}, \dots, n^{n-1} - (n-1)^{n-1},$$

die zweiten Differenzen (vergl. Serret, *Höhere Algebra*, deutsch von G. Wertheim, Bd. I, S. 270)

$$3^{n-1} - 2.2^{n-1} + 1, 4^{n-1} - 2.3^{n-1} + 2^{n-1}, \dots,$$

die dritten Differenzen

$$4^{n-1} - 3.3^{n-1} + 3.2^{n-1} - 1, \dots,$$

die $(n-1)^{\text{te}}$ Differenz endlich ist

$$(2) \quad \begin{cases} n^{n-1} - (n-1)(n-1)^{n-1} + \frac{(n-1)(n-2)}{1.2} (n-2)^{n-1} \\ - \frac{(n-1)(n-2)(n-3)}{1.2.3} (n-3)^{n-1} + \dots + 1. \end{cases}$$

Andererseits ist (1) eine arithmetische Reihe $(n-1)^{\text{ter}}$ Ordnung, ihre $(n-1)^{\text{te}}$ Differenz also $1.2.3...(n-1)$, und wir erhalten somit

$$(3) \left\{ \begin{aligned} &1.2.3\dots(n-1) = n^{n-1} - (n-1)(n-1)^{n-1} \\ &+ \frac{(n-1)(n-2)}{1.2} (n-2)^{n-1} - \frac{(n-1)(n-2)(n-3)}{1.2.3} (n-3)^{n-1} \\ &\quad + \dots + 1. \end{aligned} \right.$$

Da nun $n^{n-1} \equiv 0 \pmod{n}$ und, wenn n eine Primzahl ist, (nach dem Fermatschen Satze)

$$(n-1)^{n-1} \equiv (n-2)^{n-1} \equiv \dots \equiv 2^{n-1} \equiv 1 \pmod{n}$$

ist, so geht diese Formel über in die Kongruenz

$$(4) \left\{ \begin{aligned} &1.2.3\dots(n-1) \equiv -(n-1) + \frac{(n-1)(n-2)}{1.2} \\ &\quad - \frac{(n-1)(n-2)(n-3)}{1.2.3} + \dots + 1 \pmod{n}, \end{aligned} \right.$$

deren rechte Seite mit

$$(1-1)^{n-1} - 1, \text{ d. i. } -1$$

identisch ist. Es ist also

$$1.2.3\dots(n-1) \equiv -1 \pmod{n}.$$

Anmerkung. Mit diesem Beweise stimmt der von Laplace in Lacroix, *Traité du calcul diff. et intégral*, T. III, p. 722 gegebene ganz überein.

II. Auflösung der Kongruenz ersten Grades mit einer Unbekannten.

Es ist nach dem Fermatschen Satze

$$a^{p-1}, \text{ d. i. } a \cdot a^{p-2} \equiv 1 \pmod{p},$$

also

$$a \cdot a^{p-2} b \equiv b \pmod{p}.$$

Diese Formel läßt erkennen, daß die Kongruenz

$$a \cdot x \equiv b \pmod{p}$$

die Wurzel

$$x \equiv a^{p-2} b \pmod{p}$$

hat. (Binet, *Journal de l'École polyt.* 20, p. 289.)

Beispiel. Die Kongruenz $7x \equiv 19 \pmod{41}$ hat die Wurzel $x \equiv 7^{39} \cdot 19 \equiv 6 \cdot 19 \equiv 114 \equiv 32 \pmod{41}$. [Der Rest von 7^{39} ergibt sich auf folgende Weise: Es ist $7^3 = 343 \equiv 15$; $7^6 \equiv 15^2 \equiv 225 \equiv 20$; $7^{12} \equiv 400 \equiv 31$; $7^{24} \equiv 961 \equiv 18$; $7^{36} \equiv 31 \cdot 18 \equiv 558 \equiv 25$; $7^{39} \equiv 25 \cdot 15 \equiv 375 \equiv 6 \pmod{41}$].

Wie man mittels des verallgemeinerten Fermatschen Satzes die Kongruenz ersten Grades löst, deren Modul eine zusammengesetzte Zahl ist, wird unten in §. 88 gezeigt werden.

§. 46.

Summe der Reste der Vielfachen einer Zahl.

Lehrsatz. Wenn $r_1, r_2, \dots, r_{m-1}$ die kleinsten positiven Reste bezeichnen, welche die $m - 1$ Vielfachen einer Zahl n

$$n, 2n, 3n, \dots, (m-1)n$$

für den Modul m geben, und δ der grösste gemeinschaftliche Divisor von m und n , nämlich $m = \delta\mu$, $n = \delta\nu$ ist, so ist

$$r_1 + r_2 + r_3 + \dots + r_{m-1} = \delta^2 \cdot \frac{\mu(\mu-1)}{2}.$$

Beispiel. Es sei $m = 9$, $n = 15$, also $\delta = 3$, $\mu = 3$, so ist

$$\delta^2 \cdot \frac{\mu(\mu-1)}{2} = 3^2 \cdot \frac{3 \cdot 2}{2} = 27.$$

In der That ist mod. 9

$$\begin{aligned} 15 &\equiv 6, & 2 \cdot 15 &\equiv 3, & 3 \cdot 15 &\equiv 0, & 4 \cdot 15 &\equiv 6, \\ 5 \cdot 15 &\equiv 3, & 6 \cdot 15 &\equiv 0, & 7 \cdot 15 &\equiv 6, & 8 \cdot 15 &\equiv 3, \end{aligned}$$

und

$$3 \cdot 6 + 3 \cdot 3 = 27.$$

Beweis. Der Rest eines Vielfachen von $n = \delta\nu$ für den Modul $m = \delta\mu$ wird offenbar erhalten, indem man den Rest, den das nämliche Vielfache von ν für den Modul μ giebt, mit δ multipliziert. Es wird also auch die Summe der Reste der Zahlen

$$(1) \quad n, 2n, 3n, \dots, (m-1)n$$

für den Modul m das δ fache der Summe der Reste der Zahlen

$$(2) \quad \nu, 2\nu, 3\nu, \dots, (m-1)\nu$$

für den Modul μ sein. Der Reihe (2) können wir noch das Glied $m\nu$ beifügen, da es den Rest Null liefert, also auf die Summe der Reste keinen Einfluß hat.

Die betrachteten Vielfachen von ν zerfallen nun in folgende δ Gruppen von je μ Zahlen:

$$\begin{array}{llll}
 (1') & v, & 2v, & \dots, \mu v, \\
 (2') & (\mu + 1)v, & (\mu + 2)v, & \dots, 2\mu v, \\
 (3') & (2\mu + 1)v, & (2\mu + 2)v, & \dots, 3\mu v, \\
 & \dots & \dots & \dots \\
 (\delta') & ([\delta - 1]\mu + 1)v, & ([\delta - 1]\mu + 2)v, & \dots, \delta\mu v,
 \end{array}$$

und da die Zahlen jeder Gruppe denjenigen der ersten für den Modul μ kongruent sind, so ist die Summe der Reste aller Zahlen (2) das δ fache der Summe der Reste der ersten Gruppe. Die Zahlen der ersten Gruppe sind aber für den Modul μ inkongruent; ihre kleinsten positiven Reste stimmen also, abgesehen von der Reihenfolge, mit den Zahlen $0, 1, 2, 3, \dots, \mu - 1$ überein, haben folglich die Summe $\frac{\mu(\mu - 1)}{2}$. Die Summe der Reste

der Zahlen (2) ist somit $\delta \cdot \frac{\mu(\mu - 1)}{2}$ und diejenige der Zahlen (1)

$$\delta^2 \cdot \frac{\mu(\mu - 1)}{2}.$$

§. 47.

Anzahl der Wurzeln einer Kongruenz, deren Modul eine Primzahl ist.

Anhangsweise mögen hier einige Betrachtungen über Kongruenzen höherer Grade folgen, deren Moduln Primzahlen sind. Die allgemeine Form einer Kongruenz m^{ten} Grades ist

$$(1) \quad A_0 x^m + A_1 x^{m-1} + \dots + A_{m-1} x + A_m \equiv 0 \pmod{p}.$$

Die Koeffizienten $A_0, A_1, \dots, A_m$ sind ganze Zahlen, die nach dem Früheren als zwischen 0 und $p - 1$ oder auch zwischen $-\frac{p}{2}$ und $+\frac{p}{2}$ liegend angesehen werden können. Der Koeffizient A_0 kann nicht $\equiv 0 \pmod{p}$ sein, da sonst der Grad der Kongruenz kleiner als m sein würde. Jeder andere Koeffizient kann dagegen durch p teilbar sein, und in diesem Falle fällt das betreffende Glied von (1) weg.

Da A_0 prim zu p ist, so läßt sich immer eine Zahl k bestimmen, welche der Bedingung $A_0 k \equiv 1 \pmod{p}$ genügt. Wenn wir nun (1) mit k multiplizieren und die Koeffizienten des Resul-

tats durch ihre kleinsten Reste für den Modul p ersetzen, so erhalten wir die Kongruenz

$$(2) \quad x^m + a_1 x^{m-1} + \dots + a_{m-1} x + a_m \equiv 0 \pmod{p},$$

welche mit (1) hinsichtlich der Wurzeln vollständig übereinstimmt. Von dieser beweisen wir die folgenden Sätze, die sich mit geringfügigen Änderungen auch von (1) hätten beweisen lassen.

Lehrsatz I. Die Kongruenz m^{ten} Grades

$$(2) \quad x^m + a_1 x^{m-1} + \dots + a_{m-1} x + a_m \equiv 0 \pmod{p},$$

deren Modul eine Primzahl ist, hat höchstens m Wurzeln.

Beweis. Wir bezeichnen der Kürze wegen die linke Seite von (2) mit $f(x)$ und nehmen an, es sei α eine Wurzel der Kongruenz $f(x) \equiv 0 \pmod{p}$, also $f(\alpha)$ durch p teilbar. Wenn wir jetzt $f(x)$ durch $x - \alpha$ dividieren und den Quotienten $f_1(x)$, den Rest r nennen, so ist

$$(3) \quad f(x) = (x - \alpha)f_1(x) + r.$$

Nun ist bekanntlich der Grad des Restes einer Division um wenigstens eine Einheit niedriger als der Grad des Divisors, und da $x - \alpha$ vom ersten Grade ist, so muß r eine von x unabhängige Zahl sein. Außerdem leuchtet ein, daß $f_1(x)$ um einen Grad niedriger als $f(x)$, also ein Polynom $(m - 1)^{\text{ten}}$ Grades sein muß. Wird jetzt in (3) $x = \alpha$ gesetzt, so erhalten wir $f(\alpha) = r$, und somit ist r eine durch p teilbare ganze Zahl.

Wenn β eine zweite Wurzel von (2), also $f(\beta) \equiv 0 \pmod{p}$ ist, so folgt aus (3)

$$(\beta - \alpha)f_1(\beta) \equiv 0 \pmod{p}.$$

Da nun $\beta - \alpha$ nicht durch p teilbar ist, so muß p in dem anderen Faktor, d. i. in $f_1(\beta)$, aufgehen, mit anderen Worten: β ist eine Wurzel der Kongruenz

$$(4) \quad f_1(x) \equiv 0 \pmod{p}.$$

Jede Wurzel von (2), mit alleiniger Ausnahme von α , genügt also auch der Kongruenz (4), oder die Kongruenz (2), die vom m^{ten} Grade ist, hat höchstens eine Wurzel mehr als die Kongruenz $(m - 1)^{\text{ten}}$ Grades (4).

Nun hat die Kongruenz ersten Grades, wenn der Modul eine Primzahl ist, nach §. 34, Lehrsatz II, eine einzige Wurzel. Folg-

lich hat in diesem Falle die Kongruenz 2. Grades höchstens zwei, diejenige 3. Grades höchstens 3, allgemein diejenige m^{ten} Grades höchstens m Wurzeln.

Folgerung. — Beweis des Wilsonschen Satzes. — Eine Kongruenz m^{ten} Grades, die mehr als m inkongruente Wurzeln besitzt, ist eine identische Kongruenz, d. h. jeder ihrer Koeffizienten ist durch den Modul p teilbar.

Dieser Satz, der aus dem vorhergehenden Lehrsatz unmittelbar folgt, liefert einen sehr einfachen Beweis des Wilsonschen Satzes.

Die Kongruenz

$$(x - 1)(x - 2) \dots (x - p - 1) - (x^{p-1} - 1) \equiv 0 \pmod{p}$$

ist, da sich das Glied x^{p-1} weghebt, vom Grade $p - 2$ und hat dabei die $p - 1$ Zahlen $1, 2, 3, \dots, (p - 1)$ zu Wurzeln. Sie ist daher eine identische Kongruenz, und somit ist, wie jeder Koeffizient, das von x unabhängige Glied durch p teilbar, oder

$$1.2.3 \dots (p - 1) + 1 \equiv 0 \pmod{p}.$$

Lehrsatz II. Die Kongruenz m^{ten} Grades $f(x) \equiv 0 \pmod{p}$ kann, wenn $m > p$ sein sollte, immer durch eine gleichbedeutende Kongruenz ersetzt werden, in welcher $m < p$ ist.

Beweis. Wir dividieren $f(x)$ durch $x^p - x$ und nennen den Quotienten der Division $\varphi(x)$, den Rest, dessen Grad höchstens $p - 1$ sein wird, $\psi(x)$. Dann ist

$$f(x) = (x^p - x)\varphi(x) + \psi(x).$$

Da nun $x^p - x = x(x^{p-1} - 1)$ für jeden Wert von x durch p teilbar, also $\equiv 0 \pmod{p}$ ist, so ist $f(x) \equiv 0 \pmod{p}$ vollkommen identisch mit $\psi(x) \equiv 0 \pmod{p}$, und diese letztere Kongruenz ist höchstens vom Grade $p - 1$.

Beispiel. Um den Grad der Kongruenz

$$x^7 + 6x^5 - 3x^3 + 1 \equiv 0 \pmod{3}$$

zu erniedrigen, dividieren wir die linke Seite durch $x^3 - x$. Als Rest ergibt sich $4x + 1$. Folglich ist die vorgelegte Kongruenz identisch mit

$$4x + 1 \equiv 0 \pmod{3},$$

und diese letztere (also auch die vorgelegte) hat nur die Wurzel

$$x \equiv 2 \pmod{3}.$$

Lehrsatz III. Es seien $f(x)$, $\varphi(x)$, $\psi(x)$ Polynome, deren Koeffizienten ganze Zahlen sind, und es werde

$$f(x) = \varphi(x) \cdot \psi(x)$$

vorausgesetzt. Wenn dann die Kongruenz

$$(1) \quad f(x) \equiv 0 \pmod{p}$$

so viele inkongruente Wurzeln besitzt, wie ihr Grad Einheiten enthält, so ist dasselbe mit jeder der beiden Kongruenzen

$$(2) \quad \varphi(x) \equiv 0, \quad \psi(x) \equiv 0 \pmod{p}$$

der Fall.

Beweis. Wenn die Grade der Polynome $f(x)$, $\varphi(x)$, $\psi(x)$ beziehungsweise mit r , s , t bezeichnet werden, so ist bekanntlich $r = s + t$. Nun besitzt die Kongruenz (1) nach Voraussetzung r Wurzeln. Eine beliebige dieser Wurzeln sei α . Dann ist

$$f(\alpha) = \varphi(\alpha) \cdot \psi(\alpha) \equiv 0 \pmod{p}.$$

Es muß also mindestens einer der Faktoren $\varphi(\alpha)$, $\psi(\alpha)$ durch p teilbar sein, d. h. α ist eine Wurzel von mindestens einer der Kongruenzen (2), oder die Kongruenzen (2) besitzen zusammen nicht weniger als $r = s + t$ Wurzeln. Hätte nun eine der Kongruenzen (2) weniger Wurzeln, als ihr Grad Einheiten enthält, so müßte die andere, damit die Gesamtzahl der Wurzeln nicht unter r hinabsinkt, mehr Wurzeln haben, als ihr Grad Einheiten enthält, und das widerspricht dem Lehrsatz I.

Zusatz I. Es seien $f(x)$ und $\varphi(x)$ Polynome, deren Koeffizienten ganze Zahlen und deren Grade kleiner als die Primzahl p sind. Wenn dann $f(x)$ ein Divisor von

$$x^{p-1} - 1 + p\varphi(x)$$

ist, so besitzt die Kongruenz

$$f(x) \equiv 0 \pmod{p}$$

genau so viele Wurzeln, als ihr Grad Einheiten enthält.

Beweis. Da $f(x)$ ein Divisor von $x^{p-1} - 1 + p\varphi(x)$ ist, so können wir

$$x^{p-1} - 1 + p\varphi(x) = f(x) \cdot \psi(x)$$

annehmen, wo $\psi(x)$ ebenfalls ein Polynom ist, dessen Koeffizienten ganze Zahlen sind. Nun hat die Kongruenz $(p-1)^{\text{ten}}$ Grades

$$x^{p-1} - 1 + p\varphi(x) \equiv 0 \pmod{p}$$

die $p-1$ Zahlen $1, 2, 3, \dots, p-1$ zu Wurzeln. Folglich besitzt nach dem vorhergehenden Lehrsatz auch die Kongruenz $f(x) \equiv 0 \pmod{p}$ so viele Wurzeln, als ihr Grad Einheiten enthält.

Zusatz II. Wenn d ein Divisor von $p-1$ ist, so besitzt die Kongruenz

$$x^d \equiv 1 \pmod{p}$$

d inkongruente Wurzeln.

Beweis. Unter der gemachten Voraussetzung geht bekanntlich $x^d - 1$ in $x^{p-1} - 1$ auf, d. h. es ist

$$x^{p-1} - 1 = (x^d - 1)\varphi(x),$$

wo $\varphi(x)$ ein Polynom mit ganzen Koeffizienten bezeichnet. Daher hat nach Zusatz I die Kongruenz $x^d - 1 \equiv 0 \pmod{p}$ d Wurzeln.

Lehrsatz IV. Wenn die Polynome $f(x)$ und $\varphi(x)$ einen grössten gemeinschaftlichen Divisor $\psi(x)$ haben, so sind die den Kongruenzen

$$(1) \quad f(x) \equiv 0 \quad \text{und} \quad \varphi(x) \equiv 0 \pmod{p}$$

gemeinschaftlichen Wurzeln auch Wurzeln der Kongruenz

$$\psi(x) \equiv 0 \pmod{p}.$$

Beweis. Bezeichnen wir den Quotienten und den Rest der Division von $f(x)$ durch $\varphi(x)$ beziehungsweise mit Q und R , wo Q und R Polynome mit ganzzahligen Koeffizienten sind, so ist

$$f(x) = Q \cdot \varphi(x) + R,$$

und man erkennt leicht, daß jede den Kongruenzen (1) gemeinschaftliche Wurzel auch Wurzel der Kongruenzen

$$(2) \quad \varphi(x) \equiv 0, \quad R \equiv 0 \pmod{p}$$

sein muß. Durch Fortsetzung dieser Schlüsse findet man, daß die gemeinschaftlichen Wurzeln von (1) auch die Kongruenz $\psi(x) \equiv 0 \pmod{p}$ befriedigen müssen.

Aufgabe. Die Anzahl der Wurzeln der Kongruenz

$$(1) \quad f(x) \equiv 0 \pmod{p}$$

zu bestimmen, deren Modul p eine Primzahl ist.

Lösung. Die Kongruenz

$$(2) \quad x^{p-1} - 1 \equiv 0 \pmod{p}$$

hat die $p - 1$ Wurzeln $1, 2, 3, \dots, p - 1$. Um also die Anzahl der Wurzeln von (1) zu bestimmen, haben wir nur zu sehen, wieviele Wurzeln (1) und (2) gemeinschaftlich haben. Wir suchen somit den größten gemeinschaftlichen Divisor von

$$x^{p-1} - 1 \quad \text{und} \quad f(x).$$

Der Grad desselben giebt an, wieviele Wurzeln die Kongruenz (1) besitzt.

Beispiele. I. Um die Anzahl der Wurzeln der Kongruenz

$$(1) \quad 5x^4 - 3x^3 + 2x^2 - 6x - 2 \equiv 0 \pmod{7}$$

zu bestimmen, haben wir den größten gemeinschaftlichen Divisor von $x^6 - 1$ und $5x^4 - 3x^3 + 2x^2 - 6x - 2$ zu suchen. Damit der Quotient der zu diesem Zwecke erforderlichen Division ganzzahlige Koeffizienten erhalte, ist der Koeffizient von x^4 in (1) auf die Einheit zu reduzieren. Die Kongruenz

$$5k \equiv 1 \pmod{7}$$

hat die Wurzel $k = 3$, und durch Multiplikation mit 3 finden wir, daß die Kongruenz (1) identisch ist mit

$$(2) \quad x^4 - 2x^3 - x^2 + 3x + 1 \equiv 0 \pmod{7}.$$

Dividieren wir jetzt $x^6 - 1$ durch die linke Seite von (2), so bleibt der Rest

$$2x^3 - 2x^2 + 4x - 6 = 2(x^3 - x^2 + 2x - 3).$$

Mit $x^3 - x^2 + 2x - 3$ dividieren wir weiter in $x^4 - 2x^3 - x^2 + 3x + 1$; als Rest ergibt sich

$$-4x^3 + 8x - 2 \equiv -4x^2 + 8x - 16 = -4(x^2 - 2x + 4).$$

Wird jetzt $x^3 - x^2 + 2x - 3$ durch $x^2 - 2x + 4$ dividiert, so bleibt der Rest $-7 \equiv 0 \pmod{7}$. Die Kongruenz (1) hat daher mit $x^6 - 1 \equiv 0 \pmod{7}$ nur die Wurzeln von

$$x^2 - 2x + 4 \equiv 0 \pmod{7},$$

d. i. $x_1 \equiv 3, x_2 \equiv 6$ gemeinschaftlich, mit anderen Worten: die Kongruenz (1) besitzt nur die Wurzeln 3 und 6.

II. Die Kongruenz

$$5x^4 - x^3 + 2x^2 + 4x - 1 \equiv 0 \pmod{11}$$

hat die beiden Wurzeln

$$x_1 \equiv 5, \quad x_2 \equiv 3 \pmod{11};$$

denn als größter gemeinschaftlicher Divisor von $x^{10} - 1$ und $5x^4 - x^3 + 2x^2 + 4x - 1$ ergibt sich $x^2 - 8x + 4$, und es ist $x^2 - 8x + 4 \equiv (x - 4)^2 - 12 \equiv (x - 4)^2 - 1 \pmod{11}$. Die gesuchten Wurzeln sind also die Wurzeln der Kongruenz $(x - 4)^2 \equiv 1 \pmod{11}$, und diese liefert $x - 4 \equiv \pm 1$, also

$$x_1 \equiv 5, \quad x_2 \equiv 3 \pmod{11}.$$

Viertes Kapitel.

Einige unbestimmte Gleichungen höherer Grade. — Die Gleichung $x^y = y^x$. — Aufgaben.

§. 48.

Auflösung der unbestimmten Gleichung zweiten Grades mit zwei Unbekannten, von denen die eine nur im ersten Grade vorkommt.

Um die Gleichung

$$ax + by + cxy + dy^2 + e = 0,$$

deren Koeffizienten a, b, c, d, e ganze Zahlen sind, in ganzen Zahlen zu lösen, entnehmen wir aus derselben den Wert von x :

$$x = -\frac{dy^2 + by + e}{cy + a}.$$

Damit nun bei Ausführung der hier geforderten Division die Koeffizienten des Quotienten ganze Zahlen werden, berechnen wir, wenn c von 1 verschieden ist, zunächst den Ausdruck

$$c^2x = -\frac{c^2dy^2 + bc^2y + c^2e}{cy + a}.$$

Es ergebe sich

$$c^2x = \alpha y + \beta + \frac{\gamma}{cy + a},$$

wo α, β, γ ganze Zahlen sind. Damit nun c^2x eine ganze Zahl werde, muß $cy + a$ in γ aufgehen. Jeder Divisor δ von γ , für welchen sich aus der Gleichung

$$cy + a = \delta$$

ein ganzer Wert von y ergibt, liefert einen ganzen Wert von c^2x . Von den Werten, die so für c^2x erhalten werden, sind natürlich nur die durch c^2 teilbaren, also diejenigen zu nehmen, für welche auch x eine ganze Zahl wird.

Beispiele. I. Aus der Gleichung

$$7x - 3xy - 5y + 4y^2 = 19$$

folgt

$$x = \frac{-4y^2 + 5y + 19}{-3y + 7}$$

oder

$$9x = \frac{36y^2 - 45y - 171}{3y - 7}$$

Die Ausführung der Division liefert

$$9x = 12y + 13 - \frac{80}{3y - 7}$$

Die Zahl 80 hat die Divisoren

$$\pm 1, \pm 2, \pm 4, \pm 5, \pm 8, \pm 10, \pm 16, \pm 20, \pm 40, \pm 80,$$

und es ergibt sich bei Fortlassung derjenigen, welche für y keine ganze Zahl liefern,

$3y - 7 = -1$	2	-4	5	8	-10	-16	20	-40	80
$y = 2$	3	1	4	5	-1	-3	9	-11	29
$9x = 117$	9	45	45	63	9	-18	117	-117	360
$x = 13$	1	5	5	7	1	-2	13	-13	40.

Die Aufgabe hat also, wenn man nur positive Werte berücksichtigt, die sieben Lösungen:

$x \dots$	1	5	5	7	13	13	40
$y \dots$	3	1	4	5	9	2	29.

II. (Bhāscara, S. Colebrooke, S. 270.)

$$4x + 3y + 2 = xy,$$

$$x(y - 4) = 3y + 2,$$

$$x = \frac{3y + 2}{y - 4} = 3 + \frac{14}{y - 4}.$$

$y - 4 \dots$	14	7	2	1	-14	-7	-2	-1
$y \dots$	18	11	6	5	-10	-3	2	3
$x \dots$	4	5	10	17	2	1	-4	-11.

Die Methode verliert ihre Anwendbarkeit, wenn $c = 0$, also

$$x = - \frac{dy^2 + by + e}{a}$$

ist. Man hat dann durch Probieren zu bestimmen, welche Werte von y ganze Werte für x liefern. Um die Zahl dieser Versuche zu verringern, erwägen wir Folgendes:

Wenn η eine ganze Zahl bezeichnet, die, für y eingesetzt, x zu einer ganzen Zahl macht, so wird auch $y = \eta + ka$, wo k eine beliebige ganze Zahl bezeichnet, x zu einer ganzen Zahl machen; denn es ist

$$d(\eta + ka)^2 + b(\eta + ka) + e = (d\eta^2 + b\eta + e) + a(2dk\eta + adk^2 + bk)$$

durch a teilbar, sobald $d\eta^2 + b\eta + e$ es ist. Wenn nun nicht schon $\eta \leq \frac{a}{2}$ ist, so können wir über k so verfügen, daß $\eta + ka \leq \frac{a}{2}$ werde. Um also alle Lösungen der Aufgabe zu finden, kann man sich darauf beschränken, die Werte für y zu prüfen, deren absoluter Betrag nicht größer als $\frac{a}{2}$ ist.

Beispiel. Aus

$$7x + 3y - 11y^2 + 3 = 0$$

folgt

$$x = \frac{11y^2 - 3y - 3}{7} = y^2 + \frac{4y^2 - 3y - 3}{7}.$$

Um zu sehen, welche Werte von y den Bruch zu einer ganzen Zahl machen, haben wir y in demselben der Reihe nach durch ± 3 , ± 2 , ± 1 , 0 zu ersetzen. Als passende Werte ergeben sich nur -3 und $+2$. Die Lösungen der Aufgabe sind also

$$y = -3 + 7k, \quad x = 15 - 69k + 77k^2$$

und

$$y = +2 + 7k, \quad x = 5 + 41k + 77k^2.$$

Wegen der Unbestimmtheit von k liefert jede derselben unendlich viele Wertepaare x, y , welche der Gleichung genügen.

Aufgabe. (Maximus Planudes, Rechenbuch, deutsch von Hermann Wäschke, S. 55.) Zwei Rechtecke von gleichem Umfange zu finden, von denen das eine an Fläche a mal so groß wie das andere sei.

Lösung. Das erste Rechteck habe die Seiten x und 1 , das zweite y und $x + 1 - y$, so soll

$$ax = xy + y - y^2,$$

also

$$x = \frac{y^2 - y}{y - a} = y + a - 1 + \frac{a(a - 1)}{y - a}$$

sein. y ist so zu wählen, daß $a(a - 1)$ durch $y - a$ teilbar werde. Das ist unter anderem der Fall, wenn $y - a = 1$ (Annahme des Planudes) oder $y - a = a$ oder $y - a = a - 1$ ist. Die erste Annahme liefert für das erste Rechteck die Seiten $a^2 + a$ und 1 , für das zweite $a + 1$ und a^2 oder allgemeiner für das erste $k(a^2 + a)$ und k , für das zweite $k(a + 1)$ und ka^2 , wo k jede ganze Zahl sein kann. Die zweite Annahme liefert für das erste Rechteck $4a - 2$ und 1 , für das zweite $2a$ und $2a - 1$. Die dritte Annahme führt zu demselben Resultat wie die zweite.

Anmerkung. Gleichungen höherer Grade mit zwei Unbekannten, von denen die eine nur im ersten Grade vorkommt, werden von Lagrange im Zusatz IV zu Eulers Algebra (Oeuvres VII, S. 95) behandelt.

§. 49.

Die Pythagoreische Gleichung.

Wir stellen uns die Aufgabe, die Gleichung

$$x^2 + y^2 = z^2,$$

die wegen ihres Zusammenhanges mit dem Pythagoreischen Lehrsatz die Pythagoreische Gleichung genannt wird, in ganzen positiven Zahlen zu lösen. Da ein gemeinschaftlicher Divisor zweier der Zahlen x, y, z auch in der dritten aufgehen müßte, also durch Division beseitigt werden könnte, so dürfen wir diese

Zahlen von vornherein als teilerfremd voraussetzen. Setzen wir jetzt

$$x^2 + y^2 = (x + ky)^2,$$

wo k eine unbestimmte rationale Zahl bezeichnet, so ergibt sich leicht

$$y = \frac{2kx}{1-k^2}; \quad z = x + ky = \frac{(1+k^2)x}{1-k^2}.$$

Die Gleichung $x^2 + y^2 = z^2$ wird also durch die Werte

$$x, \quad \frac{2kx}{1-k^2}, \quad \frac{(1+k^2)x}{1-k^2},$$

somit auch durch

$$1-k^2, \quad 2k, \quad 1+k^2$$

identisch befriedigt. Will man Lösungen in ganzen Zahlen erhalten, so setze man $k = \frac{n}{m}$, wo n, m als relative Primzahlen vorausgesetzt werden dürfen. Durch Erweiterung aller drei Werte mit m^2 ergibt sich dann als Lösung der Pythagoreischen Gleichung

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2.$$

Darin können m und n als relative Primzahlen nicht beide gerade sein. Sie können aber auch nicht beide ungerade sein, da sonst x und z , ebenso wie y es ist, gerade sein würden. Wenn wir also Lösungen ohne gemeinschaftlichen Teiler erhalten wollen, so muß eine der Zahlen m, n als gerade, die andere als ungerade angenommen werden.

Dafs sich aus jeder so gefundenen Lösung der Gleichung durch Multiplikation der erhaltenen Werte mit einer beliebigen Zahl unzählig viele andere Lösungen ergeben, leuchtet von selbst ein.

Satz. Eine der Zahlen x, y ist durch 3, eine durch 4 teilbar; weiter ist eine der Zahlen x, y, z durch 5, das Produkt xyz also durch 60 teilbar. (Bernard Frenicle de Bessy, Des triangles rectangles, Mémoires de l'Acad. royale des Sciences. T. V, Paris 1729, S. 123 ff.)

Beweis. I. Wenn eine der Zahlen m, n durch 3 teilbar ist, so ist es auch $y = 2mn$.

Ist $m \equiv n \pmod{3}$, so ist $m - n$, also auch

$$x = m^2 - n^2 \equiv 0 \pmod{3}.$$

Hat endlich eine der Zahlen m, n für den Modul 3 den Rest $+1$, die andere den Rest -1 , so ist $m+n$, also ebenfalls x durch 3 teilbar.

II. Da eine der Zahlen m, n gerade ist, so ist y durch 4 teilbar.

III. Was endlich den Modul 5 betrifft, für welchen die Reste $0, \pm 1, \pm 2$ möglich sind, so ist y durch 5 teilbar, wenn eine der Zahlen m, n es ist.

x ist durch 5 teilbar, wenn jede der Zahlen m, n den Rest 1, ebenso wenn jede den Rest 2 hat, wobei es auf das Vorzeichen nicht ankommt; denn in jedem dieser beiden Fälle ist

$$m^2 - n^2 \equiv 0 \pmod{5}.$$

Wenn dagegen eine der Zahlen m, n den Rest ± 1 , die andere den Rest ± 2 hat, so ist $m^2 + n^2$, also auch $z \equiv 0 \pmod{5}$.

Aufgabe. Die einem gegebenen Werte $x=a$ entsprechenden Werte y, z zu finden, welche der Gleichung $x^2 + y^2 = z^2$ genügen.

Lösung. Da $a^2 = z^2 - y^2 = (z+y)(z-y)$ sein soll, so denken wir uns a^2 in zwei ungleiche Faktoren zerlegt, $a^2 = \alpha\alpha'$, wo $\alpha > \alpha'$ sein möge, und setzen

$$\alpha = z + y, \quad \alpha' = z - y.$$

Dann ergibt sich

$$z = \frac{\alpha + \alpha'}{2}, \quad y = \frac{\alpha - \alpha'}{2};$$

damit also z, y ganze Zahlen werden, müssen die Faktoren α, α' von a^2 beide gerade oder beide ungerade sein.

Jede geeignete Zerlegung von a^2 liefert eine Lösung der Aufgabe.

Beispiele. I. Da

$$9^2 = 81 = 1 \cdot 81 = 27 \cdot 3$$

und

$$\frac{81+1}{2} = 41, \quad \frac{81-1}{2} = 40; \quad \frac{27+3}{2} = 15, \quad \frac{27-3}{2} = 12$$

ist, so erhalten wir

$$9^2 = 41^2 - 40^2 = 15^2 - 12^2.$$

II. Es ist

$$12^2 = 72 \cdot 2 = 36 \cdot 4 = 24 \cdot 6 = 18 \cdot 8,$$

und daraus folgt

$$12^2 = 37^2 - 35^2 = 20^2 - 16^2 = 15^2 - 9^2 = 13^2 - 5^2.$$

Anmerkung I. Wenn x, y, z teilerfremd sind, so muß $z = m^2 + n^2 \equiv 1 \pmod{4}$ sein; denn das Quadrat einer geraden Zahl ist durch 4 teilbar, und für eine ungerade Zahl $2\alpha + 1$ erhält man $(2\alpha + 1)^2 = 4\alpha^2 + 4\alpha + 1 \equiv 1 \pmod{4}$.

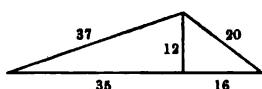
Anmerkung II. Pierre Fermat hat in seinen Zusätzen zur Arithmetik des Diophant eine Reihe schätzbarer Bemerkungen über die Pythagoreische Gleichung gemacht. Der Verfasser hat diese Zusätze in seine deutsche Übersetzung aufgenommen.

Anmerkung III. Die von Fermat in der Anm. zu Diophant II, 8 behauptete Unmöglichkeit einer rationalen Lösung der Gleichung $x^n + y^n = z^n$ für $n > 2$ ist trotz aller Bemühungen der größten Mathematiker (Euler, Dirichlet, Kummer u. a.) noch nicht allgemein bewiesen.

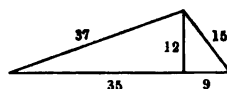
Anmerkung IV. Zahlen, für welche der von Heron von Alexandria bewiesene Ausdruck¹⁾ für die Fläche eines Dreiecks

$$J = \sqrt{s(s-a)(s-b)(s-c)}$$

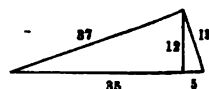
[darin bedeuten a, b, c die Seiten, s der halbe Umfang] rational ist, heißen Heronische Zahlen, und die Dreiecke selbst werden auch wohl Heronische genannt. Zwei Pythagoreische Dreiecke, die in einer Kathete übereinstimmen, lassen sich zu einem Heronischen Dreieck zusammensetzen. Danach liefert das oben gegebene Beispiel II sechs Heronische Dreiecke, nämlich



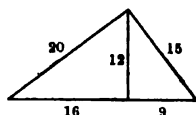
Seiten 37, 20, 51.



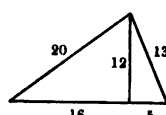
Seiten 37, 15, 44.



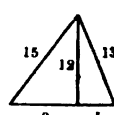
Seiten 37, 13, 40.



Seiten 20, 15, 25.



Seiten 20, 13, 21.



Seiten 15, 13, 14.

¹⁾ Vergl. Cantor, Vorlesungen über Geschichte der Mathematik Bd. I, S. 359.

§. 50.

Die Gleichung $a + bx + cx^2 = y^2$ (Euler, Algebra Bd. II, Kapitel IV).

Die Ermittlung der rationalen Werte von x , welche den Ausdruck $a + bx + cx^2$ zu einem vollständigen Quadrat oder, was dasselbe ist, $\sqrt{a + bx + cx^2}$ rational machen, ist nur ein spezieller Fall der Aufgabe, die Gleichung zweiten Grades mit zwei Unbekannten in rationalen Zahlen zu lösen. In Betreff dieser allgemeineren, von Lagrange im Zusatz V zu Eulers Algebra behandelten Aufgabe sei auf meine „Elemente der Zahlentheorie“ (B. G. Teubner, 1887), S. 226 ff. verwiesen. Hier setzen wir voraus, daß die Koeffizienten a, b, c gewissen Bedingungen genügen, welche die Sache ungemein vereinfachen und die Verwandlung des Ausdrucks $a + bx + cx^2$ in ein Quadrat immer gestatten.

1. Fall. Besonders einfach gestaltet sich die Sache, wenn einer der Koeffizienten a, c oder auch beide Null sind.

Ist erstens $a = c = 0$, so setze man

$$bx = k^2,$$

wo k eine beliebige rationale Zahl bezeichnet. Dann ergibt sich

$$x = \frac{k^2}{b}$$

als Wert von x , für welchen $\sqrt{bx}$ rational wird.

Ist zweitens $a = 0$, so setzen wir

$$bx + cx^2 = (kx)^2$$

und erhalten

$$x = \frac{b}{k^2 - c}.$$

Wenn endlich $c = 0$ ist, so liefert die Annahme

$$a + bx = k^2$$

den Wert

$$x = \frac{k^2 - a}{b}.$$

Beispiele. I. (Diophant III, 5.) Drei Zahlen zu finden, deren Summe ein Quadrat ist, und die so beschaffen

sind, daß die Summe je zweier die dritte Zahl um eine Quadratzahl übertrifft.

Diophant setzt

$$\begin{aligned} I + II + III &= x^2 + 2x + 1, \\ I + II - III &= 1, \\ -I + II + III &= x^2; \end{aligned}$$

dann erhält er

$$I = x + \frac{1}{2}, \quad II = \frac{1}{2}x^2 + \frac{1}{2}, \quad III = \frac{1}{2}x^2 + x,$$

und damit noch $I - II + III$, d. i. $2x$ ein Quadrat werde, setzt er

$$2x = 16,$$

was ihm $x = 8$, also

$$I = 8\frac{1}{2}, \quad II = 32\frac{1}{2}, \quad III = 40$$

liefert.

II. (Diophant II, 22.) Zwei Zahlen von der Beschaffenheit zu finden, daß das Quadrat einer jeden, wenn man es um die andere Zahl vermindert, eine Quadratzahl bleibt.

Diophant nimmt die kleinere Zahl $= x + 1$, die größere $= 2x + 1$ an; dann ist schon $(x + 1)^2 - (2x + 1) = x^2$ eine Quadratzahl. Es ist also nur noch zu bewirken, daß

$$(2x + 1)^2 - (x + 1) = 4x^2 + 3x$$

ein Quadrat werde. Das geschieht durch die Annahme

$$4x^2 + 3x = (3x)^2,$$

welche

$$x = \frac{3}{5}, \quad \text{also} \quad I = 1\frac{3}{5}, \quad II = 2\frac{1}{5}$$

liefert.

III. (Diophant III, 10.) Zu einer gegebenen Zahl — etwa 3 — drei andere Zahlen von der Beschaffenheit zu finden, daß die Summe je zweier der letzteren bei Addition der gegebenen Zahl ein Quadrat gebe, und daß ferner die Summe aller drei Zahlen, wenn die gegebene Zahl dazu addiert wird, ebenfalls ein Quadrat werde.

Diophant setzt

$$I + II = x^2 + 4x + 1,$$

$$II + III = x^2 + 6x + 6,$$

$$I + II + III = x^2 + 8x + 13,$$

dann ist

$$I + II + 3 = (x + 2)^2,$$

$$II + III + 3 = (x + 3)^2,$$

$$I + II + III + 3 = (x + 4)^2,$$

und man erhält

$$I = 2x + 7, \quad II = x^2 + 2x - 6, \quad III = 4x + 12.$$

Es muß nun noch

$$I + III + 3 = 6x + 22$$

zu einem Quadrat gemacht werden. Diophant nimmt

$$6x + 22 = 100$$

an. Dann erhält er $x = 13$ und

$$I = 33, \quad II = 189, \quad III = 64.$$

2. Fall. a ist eine positive Quadratzahl. Wenn $a = \alpha^2$ ist, so setzen wir

$$a + bx + cx^2 = (\alpha + kx)^2 = \alpha^2 + 2\alpha kx + k^2 x^2$$

und erhalten leicht

$$x = \frac{b^2 - 2\alpha k}{k^2 - c},$$

also, wenn $b = 0$ ist,

$$x = \frac{2\alpha k}{c - k^2}.$$

Beispiel (Diophant II, 17). Zwei Zahlen zu finden, die sich wie 1:3 verhalten, und von denen jede ein Quadrat wird, wenn man sie um die Quadratzahl 9 vergrößert.

Diophant nimmt an, die kleinere Zahl sei $x^2 + 6x$, da die eine Bedingung wegen $x^2 + 6x + 9 = (x + 3)^2$ dann schon erfüllt ist. Die größere Zahl wird $3x^2 + 18x$ sein, und die Annahme

$$3x^2 + 18x + 9 = (2x - 3)^2$$

liefert $x = 30$, so daß sich für die gesuchten Zahlen die Werte 1080 und 3240 ergeben.

3. Fall. c ist eine positive Quadratzahl. Wenn $c = \gamma^2$ ist, so setzen wir

$a + bx + cx^2 = (k + \gamma x)^2 = k^2 + 2\gamma kx + \gamma^2 x^2$
und erhalten leicht

$$x = \frac{k^2 - a}{b - 2\gamma k},$$

also, wenn $b = 0$ ist,

$$x = \frac{a - k^2}{2\gamma k}.$$

Beispiel (Diophant III, 13). Drei Zahlen von der Beschaffenheit zu finden, dafs das um 10 verminderte Produkt je zweier derselben eine Quadratzahl sei. Da sowohl $30 \frac{1}{4}$, als auch $12 \frac{1}{4}$ bei Subtraktion von 10 ein Quadrat bleibt, so nimmt Diophant

$$I = 30 \frac{1}{4} x, \quad II = \frac{1}{x}, \quad III = 12 \frac{1}{4} x$$

an. Dann sind zwei Forderungen erfüllt, und es bleibt nur noch zu bewirken, dafs $I \cdot III - 10$, d. i.

$$\frac{121 \cdot 49}{16} x^2 - 10 = \frac{121 \cdot 49 x^2 - 160}{16},$$

also $121 \cdot 49 x^2 - 160$ ein Quadrat werde. Durch die Annahme

$$121 \cdot 49 x^2 - 160 = (77x - 2)^2$$

erhält Diophant

$$x = \frac{41}{77},$$

und es ergibt sich ihm sodann

$$I = 16 \frac{3}{28}, \quad II = 1 \frac{36}{41}, \quad III = 6 \frac{23}{44}.$$

Anmerkung. Will man die Werte von x bestimmen, für welche $\sqrt{a^2 + bx + cx^2}$, z. B. $\sqrt{1 + x^2}$ rational wird, so kann man (nach Belieben) nach Fall 2 oder 3 verfahren.

4. Fall. Es ist $b^2 - 4ac$ eine Quadratzahl h^2 . In diesem Falle hat die Gleichung

$$a + bx + cx^2 = 0$$

die beiden Wurzeln

$$x_1 = \frac{-b + h}{2c}, \quad x_2 = \frac{-b - h}{2c},$$

wo $h = \sqrt{b^2 - 4ac}$ gesetzt ist. Es ergibt sich somit

$$a + bx + cx^2 = c \left(x + \frac{b-h}{2c} \right) \left(x + \frac{b+h}{2c} \right),$$

d. h. der vorgelegte Ausdruck läßt sich in zwei Faktoren ersten Grades mit rationalen Koeffizienten zerlegen.

Wir nehmen an, es sei

$$a + bx + cx^2 = (d + ex)(f + gx)$$

und setzen

$$(d + ex)(f + gx) = \frac{m^2}{n^2} (d + ex)^2,$$

wo die ganzen Zahlen m, n als prim zu einander vorausgesetzt werden. Dann ergibt sich

$$x = \frac{d m^2 - f n^2}{g n^2 - e m^2}.$$

Beispiel (Euler, Algebra II, 53). Für welche Werte von x wird $\sqrt{6 + 13x + 6x^2}$ rational? Da

$$13^2 - 4 \cdot 6 \cdot 6 = 169 - 144 = 25 = 5^2$$

ist, so unterliegt der Ausdruck dem vorliegenden Fall. Es ist

$$6 + 13x + 6x^2 = (3x + 2)(2x + 3),$$

und die Annahme

$$(3x + 2)(2x + 3) = \frac{m^2}{n^2} (3x + 2)^2$$

liefert

$$x = \frac{2m^2 - 3n^2}{2n^2 - 3m^2},$$

wo m, n irgend welche teilerfremde ganze Zahlen sind.

5. Fall. $a + bx + cx^2$ kann auf die Form $p^2 + qr$ gebracht werden, wo p, q, r Funktionen ersten Grades mit rationalen Koeffizienten bezeichnen. Wir setzen

$$p^2 + qr = \left(p + \frac{m}{n} q \right)^2,$$

wo m, n beliebige teilerfremde ganze Zahlen bezeichnen, und erhalten

$$n^2 r = 2 m n p + m^2 q,$$

aus welcher Gleichung, da sie in Beziehung auf x vom ersten Grade ist, sich x leicht bestimmen läßt.

Beispiel (Euler, Algebra II, 55). Aus $2x^2 - 1$, d. i.

$$x^2 + (x + 1)(x - 1) = \left[x + \frac{m}{n} (x + 1) \right]^2$$

ergibt sich

$$x = \frac{m^2 + n^2}{n^2 - 2mn - m^2}.$$

Für diesen Wert ist in der That

$$2x^2 - 1 = \left(\frac{m^2 - 2mn - n^2}{n^2 - 2mn - m^2} \right)^2.$$

Anmerkung. Wenn man einen Wert von x kennt, für welchen der Ausdruck $a + bx + cx^2$ ein Quadrat wird, so ist es leicht, beliebig viele andere anzugeben.

Es sei ξ ein solcher Wert und $a + b\xi + c\xi^2 = m^2$. Setzen wir dann

$$x = \xi + k,$$

wo k unbestimmt ist, so erhalten wir

$$a + bx + cx^2 = (a + b\xi + c\xi^2) + k(b + 2c\xi + ck)$$

oder

$$a + bx + cx^2 = m^2 + k(b + 2c\xi + ck).$$

Wird jetzt weiter

$$m^2 + k(b + 2c\xi + ck) = (m + kl)^2$$

gesetzt, wo l unbestimmt bleibt, so ergibt sich

$$b + 2c\xi + ck = 2ml + kl^2,$$

und hieraus folgt

$$k = \frac{2ml - b - 2c\xi}{c - l^2},$$

also

$$x = \xi + k = \frac{2ml - b - c\xi - l^2\xi}{c - l^2}.$$

Für diesen Wert von x , in welchem b, c, m, ξ bekannt sind, während l unbestimmt ist, wird $a + bx + cx^2$ ein Quadrat.

Beispiel (Diophant VI, 16). Diophant hat gefunden, daß $3.5^2 - 11$ eine Quadratzahl, nämlich 64 ist. Er will eine Quadratzahl ermitteln, die größer als 25 ist und dasselbe leistet, d. i. deren Dreifaches bei Subtraktion von 11 ein Quadrat liefere. Er nimmt die Seite des gesuchten Quadrats gleich $x + 5$ an;

dann soll $3(x + 5)^2 - 11$, d. i. $3x^2 + 30x + 64$ zu einem Quadrat gemacht werden. Zu diesem Zwecke setzt er

$$3x^2 + 30x + 64 = (8 - 2x)^2$$

und erhält

$$x = 62.$$

Die gesuchte Zahl ist also $67^2 = 4489$. In der That ist

$$3 \cdot 4489 - 11 = 13456 = 116^2.$$

Aufgaben. I. Drei Quadratzahlen gleicher Differenz zu finden, oder zwei Zahlen x, y von der Beschaffenheit zu bestimmen, daß sowohl $x^2 + y$, als auch $x^2 - y$ eine Quadratzahl sei (Leonardo Pisano Bd. II, S. 227; Lucas Paciolo, Summa fol. 46 verso; Hieronimus Cardanus, Pract. arithm. Kap. 42, Nr. 36 und 37).

Lösung. Es sei

$$\begin{aligned} x^2 + y &= a^2, \\ x^2 - y &= b^2, \end{aligned}$$

also

$$2y = a^2 - b^2 = (a + b)(a - b).$$

Setzen wir dann

$$\begin{aligned} a + b &= \frac{y}{k}, \\ a - b &= 2k, \end{aligned}$$

wo k unbestimmt ist, so erhalten wir

$$a = \frac{y}{2k} + k,$$

also

$$a^2, \text{ d. i. } x^2 + y = \frac{y^2}{4k^2} + y + k^2,$$

und daraus folgt

$$x^2 = \left(\frac{y}{2k}\right)^2 + k^2.$$

Die Zahlen $x, \frac{y}{2k}, k$ genügen demnach der Pythagoreischen Gleichung, d. h. es ist, wenn m, n teilerfremde ganze Zahlen bedeuten, von denen die eine gerade, die andere ungerade ist,

$$\begin{aligned} k &= m^2 - n^2, \\ \frac{y}{2k} &= 2mn, \end{aligned}$$

also

$$\begin{cases} y = 4mn(m^2 - n^2) \\ x = m^2 + n^2 \end{cases}$$

die Lösung der Aufgabe.

Die nachstehende Tabelle gibt Zahlen, welche der Aufgabe genügen:

<i>m</i>	<i>n</i>	<i>x</i>	<i>y</i>	Quadrate gleicher Differenz		
2	1	5	24	1,	25,	49
3	1	10	96	4,	100,	196
3	2	13	120	49,	169,	289
4	1	17	240	49,	289,	529
.	.	.	.	.	.	.

II. Eine Zahl zu finden, die sowohl bei Addition von 5, als auch bei Subtraktion von 7 eine Quadratzahl wird. (Aus dem Rechenbuch von Bakhshâli, Indian Antiquary XVII, S. 44.)
Wird

$$\begin{aligned} x + 5 &= a^2 \\ x - 7 &= b^2 \end{aligned}$$

gesetzt, so folgt

$$12 = a^2 - b^2 = (a + b)(a - b).$$

Es ist also

$$\begin{array}{l|l|l} a + b = 12 & 6 & 4 \\ a - b = 1 & 2 & 3, \end{array}$$

somit

$$\begin{array}{l|l|l} a = 6\frac{1}{2} & 4 & 3\frac{1}{2} \\ b = 5\frac{1}{2} & 2 & \frac{1}{2}, \end{array}$$

und

$$\begin{array}{l|l|l} a^2 = 42\frac{1}{4} & 16 & 12\frac{1}{4}, \\ x = 37\frac{1}{4} & 11 & 7\frac{1}{4}. \end{array}$$

III. (Diophant IV, 21.) Vier Zahlen von der Beschaffenheit zu finden, daß das Produkt je zweier derselben, wenn es um 1 vermehrt wird, ein Quadrat gebe.

Diophant nimmt

$$I = x, \quad II = x + 2, \quad III = 4x + 4, \quad IV = 9x + 6$$

an; dann sind

$$I.II + 1, I.III + 1, I.IV + 1, II.III + 1, III.IV + 1$$

Quadrate, also schon fünf Bedingungen erfüllt, und man hat nur noch $II.IV + 1$, d. i. $9x^2 + 24x + 13$ zu einem Quadrat zu machen.

Die Annahme

$$9x^2 + 24x + 13 = (3x - 4)^2$$

liefert

$$x = \frac{1}{16},$$

und so erhält Diophant für die gesuchten Zahlen die Werte

$$\frac{1}{16}, \frac{33}{16}, \frac{68}{16}, \frac{105}{16}.$$

§. 51.

Die Gleichung $ax^2 + by^2 = z^2$. (Euler, Algebra II, 188.)

Es soll

$$ax^2 + by^2 = (x\sqrt{a} + y\sqrt{-b})(x\sqrt{a} - y\sqrt{-b})$$

in einen Kubus verwandelt werden. Wenn nun x und y ohne gemeinschaftlichen Divisor sind, so muß jeder der beiden Faktoren von $ax^2 + by^2$ ein Kubus sein. Wir setzen daher

$$\begin{cases} x\sqrt{a} + y\sqrt{-b} = (p\sqrt{a} + q\sqrt{-b})^3 \\ x\sqrt{a} - y\sqrt{-b} = (p\sqrt{a} - q\sqrt{-b})^3 \end{cases}$$

und erhalten, wenn wir diese beiden Gleichungen entwickeln und die reellen und imaginären Teile einer jeden einander gleich setzen,

$$\begin{cases} x = ap^3 - 3bpq^2 \\ y = 3ap^2q - bq^3; \end{cases}$$

darin sind a, b gegeben, während p, q unbestimmt geblieben sind. Für diese Werte von x, y wird

$$ax^2 + by^2 = (ap^2 + bq^2)^3.$$

Beispiele:

$$I. \quad x^2 + y^2 = z^2.$$

Hier ist

$$x = p^3 - 3pq^2, \quad y = 3p^2q - q^3;$$

p und q sind beliebige Werte beizulegen, etwa

p	q	x	y	$x^2 + y^2$	z
1	1	- 2	2	8	2
2	1	2	11	125	5
1	2	- 11	- 2	125	5
3	1	18	26	1000	10
.	.	.	.	.	.

II.

$$x^2 + 2y^2 = z^2.$$

$$x = p^3 - 6pq^2, \quad y = 3p^2q - 2q^3.$$

p	q	x	y	$x^2 + 2y^2$	z
1	1	- 5	1	27	3
2	1	- 4	10	216	6
1	2	- 23	- 10	729	9
3	1	9	25	1331	11
.	.	.	.	.	.

Aufgabe. Beweise, daß $x^2 + 2 = z^2$ nur die eine Lösung $x^2 = 25$ hat, $x^2 + 4 = z^2$ nur die beiden Lösungen $x^2 = 4$ und $x^2 = 121$.

Diese beiden Aufgaben hatte Fermat (Varia Opera, p. 192 = Oeuvres II, S. 345) den englischen Mathematikern zur Lösung aufgegeben.

§. 52.

Die Gleichung $x^y = y^x$. (Euler, Introductio in Analysin infinitorum, II, p. 294.)

Wird $y = tx$ angenommen, so wird

$$x^{tx} = (tx)^x,$$

und daraus folgt der Reihe nach

$$x^t = t x,$$

$$x^{t-1} = t,$$

$$x = \sqrt[t-1]{t},$$

$$y = \sqrt[t-1]{t}.$$

Wenn wir jetzt $t - 1 = \frac{1}{k}$ setzen, so erhalten wir

$$x = \left(1 + \frac{1}{k}\right)^k, \quad y = \left(1 + \frac{1}{k}\right)^{k+1},$$

wo k jede rationale Zahl sein kann. Für $k = 1$ ist z. B.

$$x = 2, \quad y = 4,$$

für $k = 2$ ist

$$x = \frac{9}{4}, \quad y = \frac{27}{8};$$

u. s. w.

§. 53.

Aufgaben.

I. Welche Zahlen haben die Eigenschaft, daß ihre Quadrate und daher auch ihre sämtlichen Potenzen mit denselben Ziffern wie die Zahlen selbst endigen?

Von den einziffrigen Zahlen sind dies bekanntlich 1, 5, 6.

Um die zweiziffrigen Zahlen zu finden, nehmen wir an, es sei α eine einziffrige Zahl der verlangten Art, also entweder 1 oder 5 oder 6. Dann soll

$(10 a_1 + \alpha)^2$, d. i. $100 a_1^2 + 20 \alpha a_1 + \alpha^2 = 100 k + 10 a_1 + \alpha$ sein, wo k irgend eine ganze Zahl und $a_1 < 10$ ist. Es muß daher

$$(1) \quad 20 \alpha a_1 - 10 a_1 + \alpha^2 - \alpha = 10 a_1 (2 \alpha - 1) + \alpha (\alpha - 1)$$

ein Vielfaches von 100 sein.

Für $\alpha = 1$ ist das unmöglich. Für $\alpha = 5$ wird der Ausdruck (1) $90 a_1 + 20$, und damit dies ein Vielfaches von 100, also $9 a_1 + 2$ ein Vielfaches von 10 sei, ist $a_1 (< 10) = 2$ zu setzen.

Für $\alpha = 6$ endlich wird (1) $110 a_1 + 30$; das soll ein Vielfaches von 100, also $11 a_1 + 3$ ein Vielfaches von 10 sein, was

nur für $\alpha_1 = 7$ der Fall ist. Die zweiziffrigen Zahlen der verlangten Art sind danach 25 und 76; in der That ist

$$25^2 = 625, \quad 76^2 = 5776.$$

Um die dreiziffrigen Zahlen zu erhalten, verstehen wir unter α_1 eine zweiziffrige Zahl der verlangten Art; dann soll

$$(100\alpha_2 + \alpha_1)^2,$$

d. i.

$$10000\alpha_2^2 + 200\alpha_1\alpha_2 + \alpha_1^2 = 1000k' + 100\alpha_2 + \alpha_1,$$

also

$200\alpha_1\alpha_2 - 100\alpha_2 + \alpha_1^2 - \alpha_1 = 100\alpha_2(2\alpha_1 - 1) + \alpha_1(\alpha_1 - 1)$ ein Vielfaches von Tausend sein. Für $\alpha_1 = 25$ wird dieser Ausdruck $4900\alpha_2 + 600$, und das ist ein Vielfaches von 1000, wenn $49\alpha_2 + 6$, also auch $9\alpha_2 + 6$ ein Vielfaches von 10 ist, was nur für $\alpha_2 = 6$ der Fall ist.

Für $\alpha_1 = 76$ wird unser Ausdruck $15100\alpha_2 + 5700$, und das ist ein Vielfaches von 1000, wenn $151\alpha_2 + 57$, also auch $\alpha_2 + 7$ ein Vielfaches von 10 ist, was $\alpha_2 = 3$ liefert. Die dreiziffrigen Zahlen der betrachteten Art sind also 625 und 376, und in der That ist $625^2 = 390625$, $376^2 = 141376$.

Auf diese Weise fortschliessend erhalten wir als vierziffrige Zahlen 0625 und 9376, als fünfziffrige 90625 und 09376, als sechsziffrige 890625 und 109376, als siebenziffrige 2890625 und 7109376, u. s. w.

II. Welches ist die kleinste Zahl, die links eine 7 hat und auf ihren dritten Teil reduziert wird, wenn man diese 7 links abschneidet und rechts wieder ansetzt?

Es muß $7 \cdot 10^v = 29x + 21$ sein. Man hat also 70 durch 29 zu dividieren, an den Rest 0 zu hängen und weiter zu dividieren. In dieser Weise hat man fortzufahren, bis der Rest 21 erscheint. Der erhaltene Quotient mit vorgesetzter 7 ist die gesuchte Zahl; als solche ergibt sich

$$7241379310344827586206896551.$$

III. Eine dreiziffrige Zahl hat die Quersumme 11. Die durch Umkehrung der Reihenfolge der Ziffern gebildete Zahl würde die Hälfte der ursprünglichen sein, wenn diese um 29 größer wäre. Wie heisst die Zahl? (623)

$$100x + 10y + (11 - x - y) + 29 = 2[100(11 - x - y) + 10y + x],$$

u. s. w.

IV. Welche dreiziffrige Zahl hat sowohl im dekadischen, als auch im heptadischen System die Eigenschaft, daß jede folgende Ziffer um 1 größer ist als die vorhergehende? [123 (dekadisch) = 234 (heptadisch)].

$$100a + 10(a + 1) + (a + 2) = 49b + 7(b + 1) + (b + 2),$$

u. s. w.

V. Welche dreiziffrige Zahl wird im Elfer-System umgekehrt wie im Siebener-System geschrieben? [163 (Basis 11) = 361 (Basis 7) und 368 (Basis 11) = 863 (Basis 7)].

$$121a + 11b + c = 49c + 7b + a,$$

u. s. w.

VI. Welche zwischen 100 und 200 liegenden Zahlen endigen im Fünfezner-System mit einer 4, im Zwölfer-System mit einer 10? (Meier Hirsch, XVIII, 4.) [Es sind, dekadisch geschrieben, 34, 94, 154.]

$$15a + 4 = 144b + 12c + 10,$$

u. s. w.

VII. Welche Zahlen endigen sowohl im Fünfezner-, wie im Zwölfer-System auf 34?

$$34 \text{ im Fünfezner-System} = 49 \text{ (dekadisch),}$$

$$34 \text{ im Zwölfer-System} = 40 \text{ (dekadisch),}$$

also sind die Zahlen s zu suchen, welche den beiden Bedingungen

$$s \equiv 49 \pmod{225}, \quad s \equiv 40 \pmod{144}$$

genügen. Man erhält $s = 1624 + 3600k$, wo $k = 0$ oder jede ganze positive Zahl sein kann.

VIII. Für welche Werte von x wird jeder der Ausdrücke

$$\frac{3x - 10}{7}, \quad \frac{11x + 8}{17}, \quad \frac{16x - 1}{5}$$

eine ganze Zahl?

Für $x = 211 + 595k$, wo k jede ganze Zahl sein kann.

IX. In der augenscheinlich nicht im dekadischen System geschriebenen Rechnung

$$121m \text{ à } *2M = M4422$$

ist da, wo das Zeichen $*$ steht, eine Ziffer unleserlich. Wie heißt diese Ziffer? In welchem System ist die Rechnung geschrieben, und wie wird dieselbe im dekadischen System lauten?

Bezeichnet x die Basis des Systems und y die unleserliche Ziffer, so soll

$$(x^2 + 2x + 1)(xy + 2) = 4x^3 + 4x^2 + 12x + 2$$

sein, und daraus folgt leicht

$$y = 4 - \frac{6}{x+1}.$$

Die Lösung $x = 2$, $y = 2$ ist zu verwerfen, da es im binären System keine Ziffer 2 gibt; es kann also nur $x = 5$, $y = 3$ sein. Die Rechnung ist somit im Fünfer-System geschrieben, die unleserliche Ziffer ist 3, und die Rechnung lautet im dekadischen System

$$36m \text{ à } 17M = 612M.$$

X. Bei welchen Pythagoreischen Dreiecken verhält sich der Umfang zur Längeneinheit wie die Fläche zur Flächeneinheit?

Die Seiten des Dreiecks seien

$$x^2 + y^2, \quad x^2 - y^2, \quad 2xy;$$

dann soll

$$(x^2 - y^2)xy = 2x(x + y),$$

also

$$(x - y)y = 2 \quad \text{oder} \quad x = y + \frac{2}{y}$$

sein. Es ist also

$$\text{entweder } y = 1, \quad x = 3,$$

so daß die Seiten 10, 8, 6 sind,

$$\text{oder } y = 2, \quad x = 3,$$

so daß die Seiten 13, 5, 12 sind.

XI. Zwei ganze positive Zahlen zu finden, deren Differenz gleich dem Doppelten ihres Quotienten ist (Heis, §. 79, Nr. 30).

$$x - y = \frac{2x}{y}, \quad \text{u. s. w.}$$

$$x = y + \frac{2y}{y-2}.$$

Wir setzen $y - 2 = k$ und erhalten

$$y = 2 + k, \quad x = 4 + k + \frac{4}{k}.$$

Lösungen:

k	1	2	4
x	9	8	9
y	3	4	6

XII. Zwei ganze positive Zahlen zu finden, deren Produkt das 12fache ihrer Summe ist.

$$xy = 12(x + y), \quad x = 12 + \frac{144}{y - 12}.$$

x	156	84	60	48	36	30	24	21	y
y	13	14	15	16	18	20	24	28	x

XIII. Zwei arithmetische Reihen haben gleiche Endglieder. Die erste hat zum Anfangsglied 9 und zur Summe 25, die zweite zum Anfangsglied 8 und zur Summe 36. Wieviel Glieder hat jede Reihe? (Heis, §. 81, Nr. 22.)

Die erste Reihe habe x , die zweite y Glieder; das Endglied einer jeden sei t ; dann ist

$$\frac{(9 + t)x}{2} = 25, \quad \frac{(8 + t)y}{2} = 36,$$

und man erhält durch Elimination von t leicht

$$x = 50 - \frac{3600}{y + 72}$$

Die Betrachtung der 45 Divisoren von 3600 liefert die Lösungen:

x	2	5	10	14	20	25	26	30	32	34	35
y	3	8	18	28	48	72	78	108	128	153	168

x	38	40	41	42	44	45	46	47	48	49
y	228	288	328	378	528	648	828	1128	1728	3528

XIV. Zwei arithmetische Reihen haben gleiche Anfangsglieder. Die erste hat zum letzten Gliede 39, zur Summe 207, die zweite zum letzten Gliede 124, zur Summe 917. Wieviel Glieder hat jede Reihe? (Heis, §. 81, Nr. 21.)

Die erste Reihe habe x , die zweite y Glieder; das Anfangsglied einer jeden sei a . Dann ist

$$\frac{a+39}{2} \cdot x = 207, \quad \frac{a+124}{2} \cdot y = 917,$$

und man erhält durch Elimination von a

$$y = \frac{1834x}{85x+414}, \quad \text{also} \quad 85y = 1834 - \frac{759276}{85x+414}.$$

Die Betrachtung der 72 Divisoren von

$$759276 = 2^3 \cdot 3^2 \cdot 7 \cdot 23 \cdot 131$$

ergibt nur die eine Lösung

$$x = 9, \quad y = 14.$$

XV. Die Gleichung

$$3x + 5xy - 2y + 7y^2 = 63$$

in ganzen positiven Zahlen zu lösen.

Es ergibt sich

$$x = \frac{-7y^2 + 2y + 63}{5y + 3},$$

$$25x = \frac{-175y^2 + 50y + 1575}{5y + 3} = -35y + 31 + \frac{1482}{5y + 3}.$$

Von den Divisoren der Zahl $1482 = 2 \cdot 3 \cdot 13 \cdot 19$ hat nur einer, nämlich 13, die Eigenschaft, von der Form $5k + 3$, $k > 0$ zu sein, und es ergibt sich

$$5y + 3 = 13, \quad y = 2, \quad 25x = 75, \quad x = 3,$$

also die Lösung $x = 3$, $y = 2$.

XVI. Desgleichen die Gleichung

$$4x - 30y + 11y^2 = 25.$$

Man erhält

$$x = 6 + 7y - 3y^2 + \frac{1 + 2y + y^2}{4},$$

und daraus ergeben sich die Lösungen

$y \dots$	$1 + 4k$	$-1 + 4k$
$x \dots$	$11 + 8k - 44k^2$	$-4 + 52k - 44k^2$

Die einzigen positiven Werte, die der Gleichung genügen, enthält die zweite Lösung, die für $k = 1$

$$x = 4, \quad y = 3$$

liefert.

XVII. Es sollen ganze Werte von x, y bestimmt werden, für welche jeder der Ausdrücke

- (1) $5x^2 - 7xy + 4y^2$
- (2) $(2x + 3y)(3x - 4y)$
- (3) $2x^2 + 3xy - 2y^2$
- (4) $3x^2 - 2xy + 3y^2$

ein Quadrat wird.

Wir bestimmen die rationalen Werte von ξ , für welche jeder der Ausdrücke

- (1) $5\xi^2 - 7\xi + 4;$
- (2) $(2\xi + 3)(3\xi - 4);$
- (3) $2\xi^2 + 3\xi - 2;$
- (4) $3\xi^2 - 2\xi + 3$

ein Quadrat wird. Ist $\frac{p}{q}$ ein passender Wert von ξ und k eine beliebige ganze Zahl, so stellen $x = pk, y = qk$ Lösungen der Aufgabe dar.

XVIII. Welche gleichnamigen Brüche haben die Eigenschaft, daß ihre Differenz gleich der Differenz ihrer Kuben ist? (Meier Hirsch, XVIII, 45.)

Aus

$$\frac{m^3}{n^3} - \frac{p^3}{n^3} = \frac{m}{n} - \frac{p}{n}$$

folgt leicht

$$m^3 + mp + p^3 = n^3,$$

und die Annahme

$$m^3 + mp + p^3 = (m + kp)^3$$

liefert der Reihe nach

$$p = \frac{m(2k-1)}{1-k^2}, \quad n = m + kp = \pm \frac{m(k^2 - k + 1)}{1-k^2},$$

$$\frac{m}{n} = \pm \frac{1-k^2}{1-k+k^2}, \quad \frac{p}{n} = \pm \frac{2k-1}{1-k+k^2}.$$

XIX. Die Gleichung $x^2 + 3y^2 = z^2$ in ganzen Zahlen zu lösen.

Es ergibt sich

$$x = (3m^2 - n^2)\xi, \quad y = 2mn\xi, \quad z = (3m^2 + n^2)\xi,$$

wo m, n prim zu einander sind, während ξ unbestimmt ist.

XX. In welchen rechtwinkligen Dreiecken ist die Summe der Seiten eine Quadratzahl?

Es ist

$$[x^2 + y^2] + [x^2 - y^2] + [2xy] = 2x(x + y);$$

man hat also x, y so zu wählen, daß $2x(x + y)$ ein Quadrat werde.

XXI. Für welche Werte von x ist sowohl $x + a$, als auch $x - a$ eine Quadratzahl?

Wird $x + a = y^2$ gesetzt, so muß $x - a = y^2 - 2a$ zu einem Quadrate gemacht werden. Wir nehmen zu diesem Zwecke $y^2 - 2a = (y - k)^2$ an und erhalten

$$y = \frac{2a + k^2}{2k}, \quad x = \left(\frac{2a + k^2}{2k}\right)^2 - a = \frac{4a^2 + k^4}{4k^2}.$$

XXII. Drei ganze Zahlen bilden eine arithmetische Reihe, und je zwei derselben haben zur Summe eine Quadratzahl. Welches sind diese Zahlen?

Werden die Zahlen mit

$$x, \quad x + y, \quad x + 2y$$

bezeichnet, so soll

$$2x + y = \alpha^2, \quad 2x + 3y = \beta^2, \quad 2x + 2y = \gamma^2,$$

also

$$\alpha^2 + \beta^2 = 2\gamma^2$$

sein. Nun ist bekanntlich

$$(u + v)^2 + (u - v)^2 = 2(u^2 + v^2),$$

also, wenn $\alpha = u + v$, $\beta = u - v$ gesetzt wird,

$$\gamma^2 = u^2 + v^2$$

und nach §. 49

$$u = 2mn\xi, \quad v = (m^2 - n^2)\xi, \quad \gamma = (m^2 + n^2)\xi, \\ \alpha = (m^2 + 2mn - n^2)\xi, \quad \beta = (-m^2 + 2mn + n^2)\xi;$$

u. s. w.

XXIII. Zwei Zahlen x, y zu bestimmen, für welche sowohl $x^2 + y^2 - 1$, als auch $x^2 - y^2 - 1$ eine Quadratzahl ist (Bhāscara, Colebrooke, S. 27).

Wird

$$\begin{aligned}x^2 + y^2 - 1 &= u^2 \\x^2 - y^2 - 1 &= v^2\end{aligned}$$

gesetzt, so ist

$$2y^2 = u^2 - v^2 = (u + v)(u - v),$$

also entweder

$$(1) \quad u + v = \frac{2y}{m}, \quad u - v = my$$

oder

$$(2) \quad u + v = my^2, \quad u - v = \frac{2}{m}.$$

Die erste Annahme liefert

$$u = \frac{y}{m} + \frac{my}{2}, \quad v = \frac{y}{m} - \frac{my}{2}$$

und weiter, wenn k eine zweite unbestimmte Zahl bezeichnet,

$$\begin{aligned}y &= \frac{8km^2}{4 - 4k^2m^2 + m^4} \\x &= \frac{4 + 4k^2m^2 + m^4}{4 - 4k^2m^2 + m^4}.\end{aligned}$$

Die zweite Annahme liefert ebenso

$$y^2 = \frac{m^2 - k^2m^2 + 1}{km^3}, \quad x = \frac{m^2 + m^2k^2 + 1}{2m^2k},$$

wo m und k unbestimmt sind.

XXIV. Es sollen n ganze positive Zahlen gefunden werden, welche eine arithmetische Reihe mit der Summe n^2 bilden.

Wird das erste Glied der Reihe a , die Differenz d genannt, so soll

$$[2a + (n - 1)d] \frac{n}{2} = n^2, \quad \text{also} \quad 2a + (n - 1)d = 2n$$

sein, und man erkennt leicht, daß d nur die Werte 1, 2 haben kann.

Ist nun erstens n eine gerade Zahl, also $n - 1$ ungerade, so muß offenbar d gerade, also gleich 2 sein, und dann ergibt sich $a = 1$. Wir erhalten also die Reihe der n ersten ungeraden Zahlen 1, 3, 5, ..., $2n - 1$, deren Summe bekanntlich n^2 ist.

Ist dagegen zweitens n ungerade, also $n - 1$ gerade, so kann d sowohl 1 als auch 2 sein. Es sei $n = 2\nu + 1$; dann geht die oben hergeleitete Gleichung über in

$$a + \nu d = 2\nu + 1.$$

Für $d = 1$ folgt hieraus $a = \nu + 1$; es ergibt sich somit die Reihe

$$\nu + 1, \nu + 2, \nu + 3, \dots, 3\nu + 1,$$

d. i.

$$\frac{n+1}{2}, \frac{n+3}{2}, \dots, \frac{3n-1}{2}.$$

Für $d = 2$ wird $a = 1$, so daß wir wieder die Reihe der ungeraden Zahlen erhalten.

XXV. Welche n aufeinander folgenden ungeraden Zahlen haben zur Summe n^a ?

Die gesuchten Zahlen seien

$$2x + 1, 2x + 3, \dots, 2x + 2n - 1,$$

so soll

$$(2x + n)n = n^a, \text{ also } x = \frac{n^{a-1} - n}{2}$$

sein. Es ergeben sich somit die Zahlen

$$n^{a-1} - n + 1, n^{a-1} - n + 3, \dots, n^{a-1} + n - 1.$$

Für $a = 3$ folgt hieraus der von Nikomachos von Gerasa (*Εἰσαγωγή*, XX) gegebene Satz, nach welchem die Summe der Zahlen

$$n^2 - n + 1, n^2 - n + 3, \dots, n^2 + n - 1$$

gleich n^3 , also

$$\begin{array}{rcl} 1 & & = 1^3 \\ 3 + 5 & & = 2^3 \\ 7 + 9 + 11 & & = 3^3 \\ \dots & & \dots \end{array}$$

$$(n^2 - n + 1) + (n^2 - n + 3) + \dots + (n^2 + n - 1) = n^3$$

ist, und welcher die bekannte Formel

$$1^3 + 2^3 + 3^3 + \dots + n^3 = \left[\frac{n(n+1)}{2} \right]^2$$

liefert.

XXVI. Eine aus lauter Neunen mit angehängten Nullen gebildete Zahl zu finden, welche durch eine beliebig gegebene Zahl k teilbar ist (Annales de Mathém. de Gergonne, XIX, S. 256).

Wir dividieren die Potenzen $10, 10^2, 10^3, \dots$ durch k . Da für diesen Divisor nur die Reste $0, 1, 2, \dots, k-1$ möglich sind, so werden wir zwei Potenzen von $10, 10^m$ und 10^n finden, welche für den Modul k kongruent sind. Es sei $n > m$; dann ist

$$10^n - 10^m = 10^m(10^{n-m} - 1)$$

eine durch k teilbare Zahl, welche aus $n - m$ Neunen und m Nullen gebildet ist.

Beispiel. Für $k = 36$ ist $100 \equiv 28$ und ebenso $1000 \equiv 28$, also ist $100(10 - 1) = 900$ die gesuchte Zahl.

XXVII. Die Kanten a, b, c eines rechtwinkligen Parallelepipedes so zu bestimmen, daß die Maßzahlen der Flächen-diagonalen rational werden (Euler, Comm. arithm. coll. II, S. 650).

Es soll jede der drei Zahlen $a^2 + b^2, a^2 + c^2, b^2 + c^2$ eine Quadratzahl sein. Dies zu bewirken, setzen wir

$$a = kx - ly,$$

$$b = lx - ky,$$

$$c^2 = 4klxy.$$

Dann ist

$$a^2 + c^2 = (kx + ly)^2, \quad b^2 + c^2 = (lx + ky)^2,$$

es bleibt also nur noch $a^2 + b^2$ zu einem Quadrat zu machen. Das geschieht durch die Annahme

$$a = 2mn, \quad b = m^2 - n^2,$$

denn bei dieser ist nach §. 49 $a^2 + b^2 = (m^2 + n^2)^2$.

Nun ergibt sich aus den Gleichungen

$$kx - ly = 2mn,$$

$$lx - ky = m^2 - n^2,$$

daß

$$x = \frac{2mnk - lm^2 + ln^2}{k^2 - l^2},$$

$$y = \frac{2mnl - km^2 + kn^2}{k^2 - l^2}$$

ist, oder wenn

$$(k^2 - l^2)x = \xi, \quad (k^2 - l^2)y = \eta$$

gesetzt wird,

$$\xi = 2mnk - l(m^2 - n^2),$$

$$\eta = 2mnl - k(m^2 - n^2).$$

Jetzt muß noch

$$c^2 = 4klxy = \frac{4kl\xi\eta}{(k^2 - l^2)^2}$$

oder einfach, da 4 und $(k^2 - l^2)^2$ Quadratzahlen sind, $kl\xi\eta$ zu einem Quadrat gemacht werden. Man erhält

$$kl\xi\eta = k^2 l^2 m^4 - 2kl n(k^2 + l^2)m^3 + 2k^2 l^2 n^2 m^2 \\ + 2kl n^3(k^2 + l^2)m + k^2 l^2 n^4.$$

Wird dies gleich

$$[klm^2 - (k^2 + l^2)mn + kln^2]^2$$

gesetzt, so folgt nach leichten Reduktionen

$$4kl n = (k^2 + l^2)m.$$

Wenn wir jetzt

$$m = 4kl, \quad n = k^2 + l^2$$

annehmen, so ergibt sich

$$\xi = l(3k^2 - l^2)^2, \\ \eta = k(3l^2 - k^2)^2,$$

und weiter durch leichte Entwicklungen

$$a = kx - ly = \frac{k\xi - l\eta}{k^2 - l^2} = 8kl(k^2 + l^2),$$

$$b = lx - ky = \frac{l\xi - k\eta}{k^2 - l^2} = -k^4 + 14k^2 l^2 - l^4,$$

$$c^2 = 4kl \cdot \frac{\xi\eta}{(k^2 - l^2)^2} = \frac{4k^2 l^2}{(k^2 - l^2)^2} (3k^2 - l^2)^2 (3l^2 - k^2)^2,$$

$$c = \frac{2kl}{k^2 - l^2} (3k^2 - l^2)(3l^2 - k^2),$$

oder bei Erweiterung mit $k^2 - l^2$

$$a = 8kl(k^2 + l^2)(k^2 - l^2),$$

$$b = (-k^4 + 14k^2 l^2 - l^4)(k^2 - l^2),$$

$$c = 2kl(3k^2 - l^2)(3l^2 - k^2).$$

Beispiele:

k	l	a	b	c	a^2	b^2	c^2
2	1	240	117	-44	57 600	13 689	1 936
3	1	1 920	352	-936	3 686 400	123 904	876 096
3	2	3 120	2 035	828	9 734 400	4 141 225	685 584
4	1	8 160	-495	-4 888	66 585 600	245 025	23 892 644
4	3	16 800	11 753	10 296	282 240 000	138 133 009	106 007 616

XXVIII. Beliebige viele Quadratzahlen zu finden, deren Summe eine Quadratzahl ist.

Die Lösung erfolgt mittels der Formel

$$(a^2 - b^2)^2 + (2ab)^2 = (a^2 + b^2)^2.$$

Stellt man nämlich $a^2 + b^2$, was immer möglich ist, als Differenz zweier Quadrate dar,

$$a^2 + b^2 = a_1^2 - b_1^2,$$

so liefert jene Formel

$$(a^2 - b^2)^2 + (2ab)^2 = (a_1^2 - b_1^2)^2.$$

Ebenso ergibt sich weiter

$$(a_1^2 - b_1^2)^2 + (2a_1b_1)^2 = (a_2^2 - b_2^2)^2,$$

endlich ist

$$(a_n^2 - b_n^2)^2 + (2a_nb_n)^2 = (a_n^2 + b_n^2)^2,$$

und durch Addition aller dieser Gleichungen erhält man

$$(a^2 - b^2)^2 + (2ab)^2 + (2a_1b_1)^2 + \dots + (2a_nb_n)^2 = (a_n^2 + b_n^2)^2.$$

Beispiel. Für $a = 2$, $b = 1$ ergibt sich

$$\begin{aligned} 3^2 + 4^2 &= 5^2, \\ 5^2 + 12^2 &= 13^2, \\ 13^2 + 84^2 &= 85^2, \\ 85^2 + 3612^2 &= 3613^2, \end{aligned}$$

also ist

$$3^2 + 4^2 + 12^2 + 84^2 + 3612^2 = 3613^2.$$

Fünftes Kapitel.

Die Kettenbrüche und ihre Anwendung auf die Zahlenlehre.

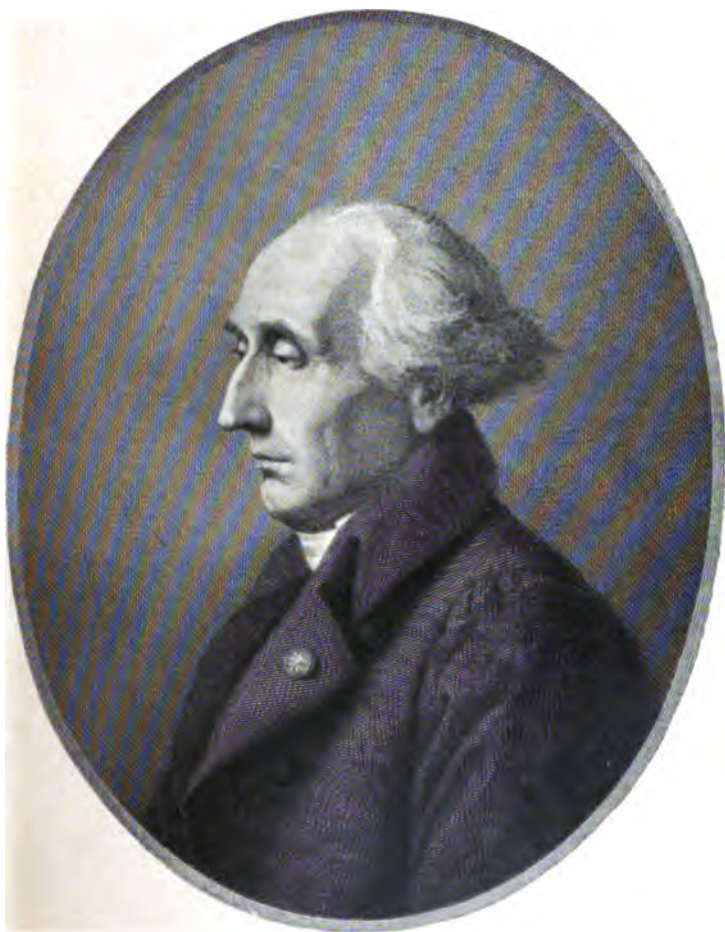
§. 54.

Historisches. — Entstehung der Kettenbrüche.

Als (erster) Erfinder der Kettenbrüche ist der Italiener Rafaele Bombelli anzusehen, der S. 35 seiner 1572 in Bologna gedruckten „Algebra“ gezeigt hat, wie man sich durch eine Kettenbruchentwicklung dem Werte einer irrationalen Quadratwurzel beliebig nähern kann. Sein Verfahren hat sich Pietro Antonio Cataldi angeeignet. Er hat dasselbe, ohne Bombelli zu nennen, dessen Werk er als Professor der Mathematik in Bologna kennen mußte, in seinem „Trattato del modo brevissimo di trovare la radice quadra delli numeri“ (Bologna 1613) weitläufig an sehr vielen Beispielen auseinander gesetzt. Dabei hat er die Eigenschaften der Näherungsbrüche entdeckt und für die Kettenbrüche eine passende, der unserigen ähnliche Bezeichnungsweise ersonnen.

Als zweiter selbständiger Erfinder ist der Nürnberger Daniel Schwenter, Professor in Altdorf, zu nennen, der sich 1618 der Kettenbrüche bediente, um das Verhältnis zweier Zahlen in kleineren Zahlen auszudrücken. So findet er (*Geometriae practicae novae* Tract. II, p. 59) für $\frac{177}{233}$ die Näherungsbrüche

$$\frac{79}{104}, \frac{19}{25} \text{ und } \frac{3}{4}.$$



Joseph Louis Lagrange

(1736 — 1812).

Nach einem Stich von Ach. Martinet.

Zum dritten Male wurden dann die Kettenbrüche von dem Engländer Lord William Brouncker (1620—1684) erfunden, der das von Wallis gegebene unendliche Produkt für $\frac{4}{\pi}$ in einen Kettenbruch verwandelte:

$$\frac{4}{\pi} = \frac{3 \cdot 3 \cdot 5 \cdot 5 \cdot 7 \cdot 7 \dots}{2 \cdot 4 \cdot 4 \cdot 6 \cdot 6 \cdot 8 \dots} = 1 + \frac{1}{2} + \frac{9}{2} + \frac{25}{2} + \frac{49}{2} + \dots$$

Wie Brouncker zu diesem Resultat gelangt ist, ist freilich nicht genau bekannt¹⁾.

Die Entstehungsweise und das Wesen der Kettenbrüche hat Lagrange in dem ersten Zusatz zu Eulers Algebra (Oeuvres, T. II, p. 8) so klar auseinander gesetzt, daß ich es für zweckmäßig halte, die betreffenden Seiten in wörtlicher Übersetzung hier folgen zu lassen:

„Unter einem Kettenbruch versteht man im allgemeinen jeden Ausdruck von der Form

$$\alpha + \frac{b}{\beta + \frac{c}{\gamma + \frac{d}{\delta + \dots}}},$$

wo die Größen $\alpha, \beta, \gamma, \delta, \dots$ und $b, c, d, \dots$ positive oder negative ganze Zahlen sind. Wir werden hier aber nur solche Kettenbrüche betrachten, in welchen jeder der Zähler $b, c, d, \dots$ die Einheit ist, welche also die Form

$$\alpha + \frac{1}{\beta + \frac{1}{\gamma + \frac{1}{\delta + \dots}}}$$

haben, wo $\alpha, \beta, \gamma, \delta, \dots$ irgend welche positive oder negative ganze Zahlen sind; denn nur diese Kettenbrüche sind in der Mathematik von erheblichem Nutzen....

„Die Kettenbrüche bieten sich uns naturgemäfs jedesmal dar, wo es sich darum handelt, gebrochene oder irrationale

¹⁾ Brounckers Resultat ist mitgeteilt und herzuleiten versucht von John Wallis in dessen Arithmetica Infinitorum (Werke 1696—1699, I, S. 470 ff.).

Größen in Zahlen auszudrücken. Nehmen wir nämlich an, wir hätten den Wert einer beliebigen gegebenen GröÙe a anzugeben, die nicht durch eine ganze Zahl ausgedrückt werden kann, so wird der einfachste Weg darin bestehen, daß wir zunächst diejenige ganze Zahl aufsuchen, welche dem Werte von a am nächsten liegt, sich also von demselben nur durch einen Bruch unterscheidet, der kleiner als 1 ist. Diese ganze Zahl sei α , so ist $a - \alpha$ gleich einem Bruche, der kleiner als 1 ist, folglich $\frac{1}{a - \alpha}$ eine Zahl, die größer als 1 ist. Es sei $\frac{1}{a - \alpha} = b$. Da b größer als die Einheit ist, so kann man wieder die ganze Zahl bestimmen, welche dem Werte von b am nächsten liegt. Wird diese ganze Zahl β genannt, so ist wieder $b - \beta$ gleich einem Bruche, der kleiner als die Einheit, folglich $\frac{1}{b - \beta}$ eine Zahl, die größer als 1 ist, und die man mit c bezeichnen kann. Um den Wert von c zu ermitteln, hat man nur die demselben am nächsten liegende ganze Zahl zu suchen. Wird dieselbe mit γ bezeichnet, so ist $c - \gamma$ kleiner als 1, folglich $\frac{1}{c - \gamma}$ eine GröÙe d , die größer als 1 ist, u. s. w. Durch dieses Verfahren muß man offenbar dem Werte von a nach und nach immer näher kommen, und zwar auf die einfachste und schnellste Weise, die möglich ist, da man nur ganze Zahlen anwendet, von denen jede dem gesuchten Werte so nahe wie möglich liegt.

„Da jetzt

$$\frac{1}{a - \alpha} = b$$

ist, so hat man

$$a - \alpha = \frac{1}{b},$$

also

$$a = \alpha + \frac{1}{b};$$

ebenso folgt aus

$$\frac{1}{b - \beta} = c, \quad \text{daß} \quad b = \beta + \frac{1}{c}$$

ist, und aus

$$\frac{1}{c - \gamma} = d, \quad \text{daß} \quad c = \gamma + \frac{1}{d}$$

ist, u. s. w., so daß man durch Einsetzung dieser Werte der Reihe nach

$$\begin{aligned} a &= \alpha + \frac{1}{b} \\ &= \alpha + \frac{1}{\beta} + \frac{1}{c} \\ &= \alpha + \frac{1}{\beta} + \frac{1}{\gamma} + \frac{1}{d} \end{aligned}$$

und allgemein

$$a = \alpha + \frac{1}{\beta} + \frac{1}{\gamma} + \frac{1}{\delta} + \dots$$

erhält.

„Es ist gut zu beachten, daß jede der Zahlen $\alpha, \beta, \gamma, \dots$, welche, wie wir eben gesehen haben, die den Gröfsen $a, b, c, \dots$ am nächsten liegenden ganzzahligen Werte sind, auf zwei verschiedene Arten genommen werden kann, da jede gegebene reelle Gröfse, die nicht selbst eine ganze Zahl ist, zwischen zwei aufeinander folgenden ganzen Zahlen liegt, von denen man jede als angenäherten Wert jener Gröfse wählen kann. Hinsichtlich des sich daraus ergebenden Kettenbruchs besteht aber zwischen den beiden Arten, diese Näherungswerte zu wählen, ein wesentlicher Unterschied. Nimmt man nämlich als Näherungswerte immer diejenigen ganzen Zahlen, welche kleiner als die wahren Werte sind, so werden die Nenner $\beta, \gamma, \delta, \dots$ sämtlich positiv sein. Dieselben werden sämtlich negativ sein, wenn man als Näherungswerte immer die ganzen Zahlen nimmt, welche gröfser als die wahren Werte sind, und sie werden zum Teil positiv, zum Teil negativ sein, wenn man bald zu kleine, bald zu grofse Näherungswerte wählt.

„Wenn nämlich α kleiner als a ist, so ist $a - \alpha$ eine positive Gröfse; folglich wird b und ebenso auch β positiv sein. Wenn dagegen α gröfser als a ist, so ist $a - \alpha$ negativ; folglich werden auch b und β negativ sein. Ebenso wird $b - \beta$ positiv sein, wenn β kleiner als b ist; in diesem Falle werden also auch c und γ positiv sein. Wenn aber β gröfser als b ist, so ist $b - \beta$

eine negative Gröfse, so dafs c und folglich auch γ negativ sein werden; u. s. w.

„Übrigens verstehe ich, wenn es sich um negative Gröfsen handelt, unter kleineren Gröfsen diejenigen, welche, positiv genommen, die gröfseren sein würden. Wir werden in der Folge zuweilen auch Gelegenheit haben, Gröfsen lediglich nach ihrem absoluten Werte zu vergleichen; wir werden dann aber nicht versäumen, darauf aufmerksam zu machen, dafs man von den Vorzeichen absehen soll.

„Ich mufs noch bemerken, dafs, wenn sich unter den Gröfsen $b, c, d, \dots$ eine befindet, die eine ganze Zahl ist, der Kettenbruch beendet sein wird, weil man diese Gröfse selbst in demselben beibehalten kann. Wenn z. B. c eine ganze Zahl ist, so wird

$$a = \alpha + \frac{1}{\beta} + \frac{1}{c}$$

der Kettenbruch sein, welcher den Wert von a liefert. Es ist nämlich klar, dafs man $\gamma = c$ nehmen müfste; dies würde

$$d = \frac{1}{c - \gamma} = \frac{1}{0} = \infty,$$

folglich

$$\delta = \infty$$

geben, so dafs man

$$a = \alpha + \frac{1}{\beta} + \frac{1}{\gamma} + \frac{1}{\infty}$$

hätte. Die folgenden Glieder werden Null, und da

$$\frac{1}{\infty} = 0$$

ist, so erhält man einfach

$$a = \alpha + \frac{1}{\beta} + \frac{1}{c}.$$

Dieser Fall wird immer eintreten, wenn die Gröfse a kommensurabel, d. h. wenn sie durch einen rationalen Bruch ausgedrückt ist. Wenn a dagegen eine irrationale oder eine transcendente Gröfse ist, so wird der Kettenbruch notwendig ins Unendliche fortgehen.“

§. 55.

Verwandlung eines rationalen Bruchs in einen Kettenbruch.

„Wir nehmen an, die GröÙe a sei ein gemeiner Bruch $\frac{A}{B}$, wo A und B gegebene ganze Zahlen sind. Die ganze Zahl α , die dem Werte von $\frac{A}{B}$ am nächsten liegt, ist offenbar der Quotient der Division von A durch B . Wir setzen voraus, diese Division sei auf die gewöhnliche Weise ausgeführt, und nennen den Quotienten α , den Rest C ; dann ist

$$\frac{A}{B} - \alpha = \frac{C}{B},$$

folglich

$$b = \frac{B}{C}.$$

„Um ebenso die ganze Zahl β zu erhalten, die dem Werte von $\frac{B}{C}$ am nächsten liegt, haben wir nur B durch C zu dividieren und als β den Quotienten dieser Division zu nehmen. Wird der Rest der Division D genannt, so ist

$$b - \beta = \frac{D}{C},$$

folglich

$$c = \frac{C}{D}.$$

„Wir werden also weiter C durch D dividieren; der Quotient dieser Division wird der Wert der Zahl γ sein, u. s. w. Daraus ergibt sich folgende einfache Regel zur Verwandlung gemeiner Brüche in Kettenbrüche:

„Man dividire zuerst den Zähler des vorgelegten Bruches durch seinen Nenner und nenne den Quotienten α ; darauf dividire man den Nenner durch den Rest und nenne den Quotienten β . Dann dividire man den ersten Rest durch den zweiten; der

Quotient sei γ . So fahre man fort, indem man immer den vorletzten Rest durch den letzten dividirt, bis man zu einer Division gelangt, die keinen Rest liefert. Das muß endlich einmal geschehen, da die Reste ganze Zahlen sind, von denen jede folgende kleiner als die vorhergehende ist. Man erhält auf diese Weise den Kettenbruch

$$\alpha + \frac{1}{\beta + \frac{1}{\gamma + \frac{1}{\delta + \dots}}}$$

der gleich dem gegebenen Bruch sein wird.

„Es sei aufgegeben, den Bruch $\frac{1103}{887}$ in einen Kettenbruch zu verwandeln. Man wird also 1103 durch 887 dividieren, was den Quotienten 1 und den Rest 216 giebt. Weiter wird man 887 durch 216 dividieren und als Quotienten 4, als Rest 23 erhalten. Dann wird man 216 durch 23 dividieren, was den Quotienten 9 und den Rest 9 giebt. Die Division von 23 durch 9 liefert sodann den Quotienten 2 und den Rest 5, die Division von 9 durch 5 den Quotienten 1 und den Rest 4, die Division von 5 durch 4 den Quotienten 1 und den Rest 1, endlich die Division von 4 durch 1 den Quotienten 4 und den Rest Null, so daß jetzt die Operation beendet ist. Stellt man nun die gefundenen Quotienten in der Reihenfolge, wie sie sich ergeben haben, zusammen, so erhält man die Reihe

$$1, 4, 9, 2, 1, 1, 4,$$

und daraus wird man den Kettenbruch bilden:

$$\frac{1103}{887} = 1 + \frac{1}{4 + \frac{1}{9 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{4}}}}}}$$

„Da man bei dem gewöhnlichen Divisionsverfahren als Quotienten immer die ganze Zahl nimmt, welche gleich dem vorgelegten Bruche oder kleiner als derselbe ist, so führt die vorhergehende Methode offenbar nur zu solchen Kettenbrüchen, deren Nenner sämtlich positive Zahlen sind.

„Wenn der Wert des Bruches nicht gleich einer ganzen Zahl ist, so kann man als Quotienten auch die ganze Zahl nehmen, welche — größer als dieser Wert — demselben unmittelbar folgt. Zu diesem Zwecke hat man den auf die gewöhnliche Weise gefundenen Quotienten nur um eine Einheit zu vergrößern. Dann wird der Rest negativ sein, und der folgende Quotient wird ebenfalls negativ sein müssen. So kann man die Glieder des Kettenbruchs nach Belieben positiv oder negativ machen.

„In dem vorhergehenden Beispiel kann man als Quotienten der Division von 1103 durch 887 statt 1 die Zahl 2 nehmen; dann wird man aber den negativen Rest — 671 erhalten, und durch diesen muß man jetzt 887 dividieren. Die Division von 887 durch — 671 ergibt den Quotienten — 1 und den Rest 216, oder den Quotienten — 2 und den Rest — 455. Nehmen wir den größeren Quotienten — 1, dann müssen wir den Rest — 671 durch den Rest 216 dividieren und erhalten entweder den Quotienten — 3 und den Rest — 23 oder den Quotienten — 4 und den Rest 193. Wir setzen die Division fort, indem wir den größeren Quotienten — 3 nehmen. Wir haben dann den Rest 216 durch den Rest — 23 zu dividieren, was entweder den Quotienten — 9 und den Rest 9 oder den Quotienten — 10 und den Rest — 14 liefert, u. s. w. Auf diese Weise erhalten wir

$$\frac{1103}{887} = 2 + \frac{1}{-1} + \frac{1}{-3} + \frac{1}{-9} + \dots,$$

wo, wie man sieht, alle Nenner negativ sind.

„Man kann übrigens jeden negativen Nenner positiv machen, indem man das Zeichen des Zählers ändert; man muß dann aber auch das Zeichen des folgenden Zählers ändern; denn es leuchtet ein, daß

$$\mu + \frac{1}{-\nu} + \frac{1}{\pi} + \dots = \mu - \frac{1}{\nu} - \frac{1}{\pi} + \dots$$

ist. Sodann kann man, wenn man will, alle Zeichen — aus dem Kettenbruch fortschaffen und ihn in einen andern verwandeln, dessen Glieder sämtlich positiv sind; denn es ist allgemein

$$\mu - \frac{1}{\nu} + \dots = \mu - 1 + \frac{1}{1} + \frac{1}{\nu-1} + \dots,$$

wie man sich leicht überzeugt, indem man beide Gröfsen in gemeine Brüche verwandelt.

„Man könnte durch ein ähnliches Mittel auch negative Glieder statt der positiven einführen; denn es ist

$$\mu + \frac{1}{\nu} + \dots = \mu + 1 - \frac{1}{1} + \frac{1}{\nu-1} + \dots$$

„Man sieht daraus, dafs man durch solche Transformationen zuweilen einen Kettenbruch vereinfachen, ihn in einen andern von kleinerer Gliederzahl verwandeln kann, und das ist allemal möglich, wenn Nenner gleich der positiven oder negativen Einheit sind.

„Im allgemeinen ist es nämlich klar, dafs, wenn man den Kettenbruch erhalten will, der sich dem Werte der gegebenen Gröfse möglichst schnell nähert, man für α , β , γ , ... immer die ganzen Zahlen wählen mufs, welche den Gröfsen a , b , c , ... am nächsten liegen, sei es dafs sie gröfser oder kleiner als dieselben sind. Nun ist es leicht zu sehen, dafs, wenn man z. B. für α nicht die ganze Zahl wählt, die der Gröfse a nach der einen oder andern Seite hin am nächsten liegt, die folgende Zahl β gleich der Einheit sein mufs; denn dann wird die Differenz $a - \alpha$ gröfser als $\frac{1}{2}$, folglich

$$b = \frac{1}{a - \alpha}$$

kleiner als 2 sein; somit wird β nur gleich 1 sein können.

„So oft man also in einem Kettenbruch Nenner findet, die gleich der Einheit sind, ist das ein Zeichen, dafs man für die vorhergehenden Nenner nicht die den Gröfsen möglichst nahe liegenden Zahlen genommen hat, und dafs somit der Kettenbruch noch vereinfacht werden kann, indem man diese Nenner um eine Einheit vergrößert oder verkleinert, was sich mittels der vorhergehenden Formeln ausführen läfst, ohne dafs es nötig wäre, die Rechnung nochmals ganz anzustellen.

„Die oben dargelegte Methode kann auch dazu benutzt werden, jede irrationale oder transcendente Gröfse, wofern man sie zuvor als Dezimalbruch ausgedrückt hat, in einen Kettenbruch zu verwandeln. Da aber der Wert in Form eines Dezimalbruchs nur ein angenäherter sein kann und man die letzte Dezi-

malstelle um eine Einheit vergrößern kann, man also zwei Grenzen erhält, zwischen denen der wahre Wert der vorgelegten GröÙe liegen muß, so wird man, um diese Grenzen nicht zu überschreiten, die Rechnung mit den beiden Brüchen, um die es sich handelt, anstellen müssen und in den Kettenbruch nur diejenigen Quotienten aufnehmen dürfen, die sich aus beiden Operationen ergeben.“

Wir werden die GröÙen $a, b, c, \dots$ die vollständigen, die ganzen Zahlen $\alpha, \beta, \gamma, \dots$ die unvollständigen Quotienten des Kettenbruchs nennen und diesen selbst der Kürze wegen zuweilen auch mit $(\alpha, \beta, \gamma, \dots)$ bezeichnen. Wenn der Wert des Kettenbruchs kleiner als 1 ist, so wird $\alpha = 0$ sein; jeder der folgenden unvollständigen Quotienten ist dagegen von Null verschieden.

Beispiele:

$$\text{I. } \frac{372}{163} = (2, 3, 1, 1, 5, 4) = (2, 4, -2, -5, -4).$$

$$\text{II. } \frac{880}{267} = (3, 3, 2, 1, 1, 1, 2, 1, 2) = (3, 3, 3, -3, 4, -3).$$

$$\text{III. } \frac{77\,708\,431}{2\,640\,858} = (29, 2, 2, 1, 5, 1, 4, 1, 1, 2, 1, 6, 1, 10, 2, 2, 3).$$

(Huygens, Opuscula posthuma. Amsterdam 1728, Bd. II, S. 174.)

$$\text{IV. } \pi = 3, 1415\,926\,535 = (3, 7, 15, 1, 292, 1, 1, \dots).$$

$$\text{V. } \frac{24x + 17}{17x + 12} = (1, 2, 2, 2, 1, x) = (2, -2, 4, -2, 2, x).$$

§. 56.

Bildung der Näherungsbrüche.

„Je mehr Glieder eines Kettenbruchs man nimmt, desto mehr wird man sich offenbar dem Werte der durch diesen Bruch ausgedrückten GröÙe nähern. Wenn man somit successive bei jedem Gliede des Bruchs inne hält, so wird man eine Reihe von GröÙen erhalten, die notwendiger Weise gegen die vorgelegte GröÙe hin konvergieren.“

„Hat man also a in den Kettenbruch

$$\alpha + \frac{1}{\beta} + \frac{1}{\gamma} + \frac{1}{\delta} + \dots$$

verwandelt, und bildet man die Größen

$$\alpha, \alpha + \frac{1}{\beta}, \alpha + \frac{1}{\beta} + \frac{1}{\gamma}, \dots$$

oder auch

$$\alpha, \frac{\alpha\beta + 1}{\beta}, \frac{\alpha\beta\gamma + \alpha + \gamma}{\beta\gamma + 1}, \dots,$$

so liegt jede folgende dem Werte von a näher als die vorhergehende.

„Um über das Bildungsgesetz und die Konvergenz dieser Größen besser urteilen zu können, bemerken wir, daß nach §. 54

$$a = \alpha + \frac{1}{b}, \quad b = \beta + \frac{1}{c}, \quad c = \gamma + \frac{1}{d}, \dots$$

ist; daraus geht hervor, daß α der erste Näherungswert von a ist. Nimmt man hierauf den wahren Wert von a , der

$$\frac{\alpha b + 1}{b}$$

ist, und ersetzt darin b durch seinen angenäherten Wert β , so erhält man den genaueren Näherungswert

$$\frac{\alpha\beta + 1}{\beta}$$

von a . Ebenso erhält man einen dritten, noch genaueren Näherungswert von a , wenn man zuerst für b seinen wahren Wert

$$\frac{\beta c + 1}{c}$$

setzt, was

$$a = \frac{(\alpha\beta + 1)c + \alpha}{\beta c + 1}$$

gibt, und darauf für c den angenäherten Wert γ schreibt. Der auf diese Weise gefundene Näherungswert von a ist

$$\frac{(\alpha\beta + 1)\gamma + \alpha}{\beta\gamma + 1}.$$

„Durch Fortsetzung dieses Schlufsverfahrens wird man sich dem Werte von a noch weiter nähern können, indem man in den oben gefundenen Ausdruck für a statt c seinen genauen

Wert $\frac{\gamma d + 1}{d}$ setzt, was

$$a = \frac{[(\alpha\beta + 1)\gamma + \alpha]d + \alpha\beta + 1}{(\beta\gamma + 1)d + \beta}$$

gibt, und darauf für d seinen angenäherten Wert δ nimmt. Man erhält so als vierte Annäherung die Gröfse

$$a = \frac{[(\alpha\beta + 1)\gamma + \alpha]\delta + \alpha\beta + 1}{(\beta\gamma + 1)\delta + \beta}$$

u. s. w.“

Wir wollen in der Folge die unvollständigen Quotienten einer in einen Kettenbruch verwandelten Gröfse a nicht mehr $\alpha, \beta, \gamma, \dots$, sondern $\alpha, \alpha_1, \alpha_2, \dots$ nennen und die Näherungsbrüche der Reihe nach mit

$$\frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \frac{P_3}{Q_3}, \dots$$

bezeichnen. Es ist also nach den obigen Entwicklungen

$$\frac{P_1}{Q_1} = \alpha, \quad \frac{P_2}{Q_2} = \frac{\alpha\alpha_1 + 1}{\alpha_1}, \quad \frac{P_3}{Q_3} = \frac{(\alpha\alpha_1 + 1)\alpha_2 + \alpha}{\alpha_1\alpha_2 + 1}, \quad \dots,$$

und aus diesen Ausdrücken entnehmen wir für das Bildungsgesetz der Näherungswerte den folgenden

Lehrsatz. Der Zähler [Nenner] des n^{ten} Näherungsbruchs wird gefunden, indem man den Zähler [Nenner] des $(n - 1)^{\text{ten}}$ Näherungsbruchs mit dem n^{ten} unvollständigen Quotienten multipliziert und zum Produkt den Zähler [Nenner] des $(n - 2)^{\text{ten}}$ Näherungsbruchs addiert.

Beweis. Nach den oben gegebenen Werten ist der Satz für den dritten Näherungsbruch richtig. Wir haben also nur zu zeigen, dafs er, wenn wir seine Geltung bis zu einer bestimmten Grenze, etwa bis zum n^{ten} Näherungsbruch, voraussetzen, auch noch für den folgenden, den $(n + 1)^{\text{ten}}$ Näherungsbruch, bestehen mufs.

Wir nehmen also an, es sei

$$\frac{P_n}{Q_n} = \frac{P_{n-1}\alpha_{n-1} + P_{n-2}}{Q_{n-1}\alpha_{n-1} + Q_{n-2}},$$

und zwar

$$\begin{aligned} P_n &= P_{n-1} \alpha_{n-1} + P_{n-2}, \\ Q_n &= Q_{n-1} \alpha_{n-1} + Q_{n-2}; \end{aligned}$$

dann ergibt sich, da der folgende Näherungsbruch dadurch erhalten wird, daß wir α_{n-1} durch $\alpha_{n-1} + \frac{1}{\alpha_n}$ ersetzen,

$$\begin{aligned} \frac{P_{n+1}}{Q_{n+1}} &= \frac{P_{n-1} \left(\alpha_{n-1} + \frac{1}{\alpha_n} \right) + P_{n-2}}{Q_{n-1} \left(\alpha_{n-1} + \frac{1}{\alpha_n} \right) + Q_{n-2}} \\ &= \frac{P_{n-1} (\alpha_{n-1} \alpha_n + 1) + P_{n-2} \alpha_n}{Q_{n-1} (\alpha_{n-1} \alpha_n + 1) + Q_{n-2} \alpha_n} \\ &= \frac{(P_{n-1} \alpha_{n-1} + P_{n-2}) \alpha_n + P_{n-1}}{(Q_{n-1} \alpha_{n-1} + Q_{n-2}) \alpha_n + Q_{n-1}}, \end{aligned}$$

also nach unserer Voraussetzung

$$\frac{P_{n+1}}{Q_{n+1}} = \frac{P_n \alpha_n + P_{n-1}}{Q_n \alpha_n + Q_{n-1}}.$$

Der Satz gilt somit für den $(n+1)^{\text{ten}}$ Näherungsbruch, wenn er für den n^{ten} richtig ist. Da er nun für den dritten besteht, so muß er auch für den vierten, weiter für den fünften, u. s. w. gelten, d. h. er hat allgemeine Geltung.

Damit sich der Geltungsbereich des Satzes auch auf den zweiten Näherungsbruch erstrecke, werden wir den fingierten Näherungsbruch

$$\frac{P_0}{Q_0} = \frac{1}{0}$$

als ersten vorausschicken; dann ist nämlich

$$\frac{P_2}{Q_2} = \frac{\alpha \alpha_1 + 1}{\alpha_1} = \frac{P_1 \alpha_1 + P_0}{Q_1 \alpha_1 + Q_0}.$$

Die Näherungsbrüche eines Kettenbruchs werden also in folgender Weise gefunden:

Man schreibt die unvollständigen Quotienten neben einander hin und setzt unter den ersten $\frac{1}{0}$, unter den zweiten $\frac{\alpha}{1}$. Darauf berechnet man der Reihe nach die Zähler [Nenner] der folgenden Näherungsbrüche, indem man den Zähler [Nenner] mit dem darüber stehenden Quotienten multipliziert und zum Produkt den Zähler [Nenner] des vorhergehenden Bruches addiert.

Beispiele (vergl. §. 55).

I.

2	3	1	1	5	4	
$\frac{1}{0}$	$\frac{2}{1}$	$\frac{7}{3}$	$\frac{9}{4}$	$\frac{16}{7}$	$\frac{89}{39}$	$\frac{372}{163}$

oder

2	4	— 2	— 5	— 4	
$\frac{1}{0}$	$\frac{2}{1}$	$\frac{9}{4}$	$\frac{-16}{-7}$	$\frac{89}{39}$	$\frac{-372}{-163}$

II.

3	3	2	1	1	1	2	1	2	
$\frac{1}{0}$	$\frac{3}{1}$	$\frac{10}{3}$	$\frac{23}{7}$	$\frac{33}{10}$	$\frac{56}{17}$	$\frac{89}{27}$	$\frac{294}{71}$	$\frac{323}{98}$	$\frac{880}{267}$

oder

3	3	3	— 3	4	— 3	
$\frac{1}{0}$	$\frac{3}{1}$	$\frac{10}{3}$	$\frac{33}{10}$	$\frac{-89}{-27}$	$\frac{-323}{-98}$	$\frac{880}{267}$

III.

29	2	2	1	5	1	. . .
$\frac{1}{0}$	$\frac{29}{1}$	$\frac{59}{2}$	$\frac{147}{5}$	$\frac{206}{7}$	$\frac{1177}{40}$	$\frac{1383}{47}$. . .

IV.

3	7	15	1	. . .
$\frac{1}{0}$	$\frac{3}{1}$	$\frac{22}{7}$	$\frac{333}{106}$	$\frac{355}{113}$. . .

Zusatz I. Jeder Näherungsbruch eines Kettenbruchs ist irreduzibel.

Beweis. P_n und Q_n können keinen gemeinschaftlichen Divisor haben, da ein solcher nach der vorhergehenden Formel auch in $(-1)^n$, also in 1 aufgehen müßte.

Zusatz II. Die Differenz zweier aufeinander folgenden Näherungsbrüche ist ein Bruch, dessen Zähler die positive oder negative Einheit und dessen Nenner das Produkt der Nenner der beiden Näherungsbrüche ist.

Beweis. Es ist

$$\frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}} = \frac{P_n Q_{n-1} - P_{n-1} Q_n}{Q_n Q_{n-1}} = \frac{(-1)^n}{Q_n Q_{n-1}}.$$

Lehrsatz II. Der Wert einer in einen Kettenbruch entwickelten GröÙe a liegt zwischen zwei aufeinander folgenden Näherungsbrüchen und zwar näher dem folgenden als dem vorhergehenden.

Beweis. Der die GröÙe a darstellende Kettenbruch habe einen vollständigen Quotienten a_n ; der entsprechende unvollständige Quotient, d. i. die gröÙste in a_n enthaltene ganze Zahl, sei α_n . Dann ist

$$\frac{P_{n+1}}{Q_{n+1}} = \frac{P_n \alpha_n + P_{n-1}}{Q_n \alpha_n + Q_{n-1}}$$

und

$$a = \frac{P_n \alpha_n + P_{n-1}}{Q_n \alpha_n + Q_{n-1}};$$

daraus ergibt sich

$$\begin{aligned} \frac{P_n}{Q_n} - a &= \frac{P_n}{Q_n} - \frac{P_n \alpha_n + P_{n-1}}{Q_n \alpha_n + Q_{n-1}} = \frac{P_n Q_{n-1} - P_{n-1} Q_n}{Q_n (Q_n \alpha_n + Q_{n-1})} \\ &= \frac{(-1)^n}{Q_n (Q_n \alpha_n + Q_{n-1})}. \end{aligned}$$

Ebenso erhält man

$$a - \frac{P_{n-1}}{Q_{n-1}} = \frac{(P_n Q_{n-1} - P_{n-1} Q_n) \alpha_n}{Q_{n-1} (Q_n \alpha_n + Q_{n-1})} = \frac{(-1)^n \alpha_n}{Q_{n-1} (Q_n \alpha_n + Q_{n-1})}.$$

Da somit die beiden Differenzen

$$\frac{P_n}{Q_n} - a \quad \text{und} \quad a - \frac{P_{n-1}}{Q_{n-1}}$$

dasselbe Vorzeichen haben, so liegt a zwischen den Näherungsbrüchen $\frac{P_n}{Q_n}$ und $\frac{P_{n-1}}{Q_{n-1}}$. Da ferner $a_n > 1$ und zugleich $Q_n > Q_{n-1}$ ist, so ist der absolute Wert der ersten Differenz kleiner als der der zweiten, d. h. a liegt näher an $\frac{P_n}{Q_n}$ als an $\frac{P_{n-1}}{Q_{n-1}}$.

Nun ist

$$\frac{P_0}{Q_0} = \frac{1}{0} = \infty,$$

also $> a$ und $\frac{P_1}{Q_1} = \frac{\alpha}{1}$, also $< a$; folglich muß

$$\frac{P_2}{Q_2} > a, \quad \frac{P_3}{Q_3} < a$$

sein, u. s. w. Die Brüche

$$\frac{P_0}{Q_0}, \quad \frac{P_2}{Q_2}, \quad \frac{P_4}{Q_4}, \dots$$

bilden somit eine fallende, die Brüche

$$\frac{P_1}{Q_1}, \quad \frac{P_3}{Q_3}, \dots$$

eine steigende Reihe; beide Reihen nähern sich, je weiter man sie fortsetzt, immer mehr dem Werte von a , ohne denselben überschreiten zu können.

Zusatz I. Die Differenz zwischen einer Gröfse a und ihrem Näherungsbruch $\frac{P_{n-1}}{Q_{n-1}}$ ist dem absoluten Werte nach gröfser als

$$\frac{1}{Q_{n-1}(Q_n + Q_{n-1})}$$

und kleiner als

$$\frac{1}{Q_{n-1} Q_n},$$

also um so mehr kleiner als $\frac{1}{Q_{n-1}^2}$.

Beweis. Es ist

$$a - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)^n a_n}{Q_{n-1}(Q_n a_n + Q_{n-1})} = \frac{(-1)^n}{Q_{n-1} \left(Q_n + \frac{Q_{n-1}}{a_n} \right)}.$$

Da nun $1 < \alpha_n < \infty$ ist, so muß die Differenz

$$a - \frac{P_{n-1}}{Q_{n-1}}$$

zwischen

$$\frac{(-1)^n}{Q_{n-1}(Q_n + Q_{n-1})} \quad \text{und} \quad \frac{(-1)^n}{Q_{n-1}Q_n}$$

liegen. Der letztere, d. i. der obere Grenzwert, wird aber noch vergrößert, indem man seinen Nenner verkleinert, und das geschieht, wenn Q_n durch Q_{n-1} ersetzt wird.

Zusatz II. Es läßt sich immer ein Näherungsbruch $\frac{P_{n-1}}{Q_{n-1}}$ der irrationalen GröÙe a von der Beschaffenheit angeben, daß die Differenz

$$a - \frac{P_{n-1}}{Q_{n-1}}$$

kleiner als eine beliebig gegebene GröÙe α sei.

Beweis. Die Differenz

$$a - \frac{P_{n-1}}{Q_{n-1}}$$

ist kleiner als

$$\frac{(-1)^n}{Q_{n-1}^2};$$

sie wird daher $< \alpha$ sein, wenn

$$\frac{1}{Q_{n-1}^2} < \alpha,$$

also

$$Q_{n-1}^2 > \frac{1}{\alpha}$$

d. h.

$$Q_{n-1} > \sqrt{\frac{1}{\alpha}}$$

ist, und da die Nenner der Näherungsbrüche eine steigende Reihe bilden, so läßt sich dieser Bedingung immer genügen.

Lehrsatz III. Wenn der Wert eines irreduzibelen Bruches $\frac{A}{B}$ zwischen zwei aufeinander folgenden Näherungsbrüchen $\frac{P_{n-1}}{Q_{n-1}}$ und $\frac{P_n}{Q_n}$ liegt, so ist sein

Nenner größer als der Nenner jedes der beiden Näherungsbrüche.

Beweis. Es ist entweder

$$\frac{P_{n-1}}{Q_{n-1}} > \frac{A}{B} > \frac{P_n}{Q_n}$$

oder

$$\frac{P_{n-1}}{Q_{n-1}} < \frac{A}{B} < \frac{P_n}{Q_n}.$$

In dem einen wie in dem andern Falle haben die Differenzen

$$\frac{P_{n-1}}{Q_{n-1}} - \frac{A}{B}, \quad \frac{P_{n-1}}{Q_{n-1}} - \frac{P_n}{Q_n}$$

dasselbe Vorzeichen, und der absolute Wert der ersten Differenz ist kleiner als der der zweiten, also, wenn wir den absoluten Wert einer GröÙe dadurch ausdrücken, daß wir dieselbe in eine eckige Klammer setzen,

$$\left[\frac{P_{n-1}}{Q_{n-1}} - \frac{A}{B} \right] < \left[\frac{P_{n-1}}{Q_{n-1}} - \frac{P_n}{Q_n} \right].$$

Hieraus folgt nach §. 57, Lehrsatz I

$$\left[\frac{B \cdot P_{n-1} - A \cdot Q_{n-1}}{B \cdot Q_{n-1}} \right] < \left[\frac{1}{Q_{n-1} Q_n} \right]$$

und weiter

$$[B \cdot P_{n-1} - A \cdot Q_{n-1}] < \left[\frac{B}{Q_n} \right].$$

Die linke Seite dieser Ungleichung ist eine der Voraussetzung nach von Null verschiedene ganze Zahl; folglich muß $B > Q_n$ und um so mehr $B > Q_{n-1}$ sein.

§. 58.

Eingeschaltete Näherungsbrüche.

Es seien

$$\frac{P_{n-1}}{Q_{n-1}} \quad \text{und} \quad \frac{P_{n+1}}{Q_{n+1}}$$

zwei aufeinander folgende Glieder einer der beiden Reihen, in welche sich nach §. 57, Lehrsatz II die Näherungsbrüche eines

Kettenbruchs teilen lassen. Beide Glieder können durch den Ausdruck

$$\frac{k P_n + P_{n-1}}{k Q_n + Q_{n-1}}$$

dargestellt werden, und zwar entspricht dem Werte $k = 0$ der Bruch $\frac{P_{n-1}}{Q_{n-1}}$, dem Werte $k = \alpha_n$ der Bruch $\frac{P_n \alpha_n + P_{n-1}}{Q_n \alpha_n + Q_{n-1}}$, d. i. nach §. 56 $\frac{P_{n+1}}{Q_{n+1}}$. Wenn der unvollständige Quotient $\alpha_n > 1$ ist, so können wir der unbestimmten Zahl k außer 0 und α_n auch noch die Werte

$$1, 2, 3, \dots, \alpha_n - 1$$

beilegen; dadurch erhalten wir $\alpha_n - 1$ zwischen

$$\frac{P_{n-1}}{Q_{n-1}} \quad \text{und} \quad \frac{P_{n+1}}{Q_{n+1}}$$

liegende neue Brüche, welche eingeschaltete Näherungsbrüche genannt werden.

Wir haben in §. 57 gesehen, daß die Näherungsbrüche gerader Ordnung

$$\frac{P_0}{Q_0}, \frac{P_2}{Q_2}, \frac{P_4}{Q_4}, \dots$$

eine fallende, diejenigen ungerader Ordnung

$$\frac{P_1}{Q_1}, \frac{P_3}{Q_3}, \dots$$

eine steigende Reihe bilden, und daß beide Reihen sich dem Werte der in den Kettenbruch entwickelten GröÙe a unbegrenzt nähern. Man kann nun jede dieser Reihen vervollständigen, indem man zwischen je zwei aufeinander folgende Glieder die neuen Brüche in der Weise einschaltet, daß ihre Nenner eine Reihe wachsender Zahlen bilden. Von diesen vervollständigten Reihen läßt sich dann beweisen:

1) Daß die Differenz zweier aufeinander folgenden Glieder dem absoluten Werte nach gleich der Einheit, dividiert durch das Produkt der beiden Nenner ist.

2) Daß jede Reihe, die eine zu-, die andere abnehmend, zu dem Werte des Kettenbruchs hin konvergiert.

3) Daß, wenn ein Bruch $\frac{A}{B}$ zwischen zwei aufeinander folgenden

Gliedern einer der beiden Reihen liegt, sein Nenner B gröfser als der Nenner jedes der ihn einschließenden Brüche ist.

Die Beweise dieser Sätze übergehe ich, da sie den Beweisen der für die eigentlichen Näherungsbrüche geltenden entsprechenden Sätze ganz ähnlich sind. Der Deutlichkeit halber lasse ich zwei Beispiele folgen:

I. Beispiel.

$$\frac{1216}{531} = (2, 3, 2, 4, 3, 5).$$

Näherungsbrüche:

2	3	2	4	3	5	
$\frac{1}{0}$	$\frac{2}{1}$	$\frac{7}{3}$	$\frac{16}{7}$	$\frac{71}{31}$	$\frac{229}{100}$	$\frac{1216}{531}$

A. Die fallende Reihe ist

$$\frac{1}{0}, \frac{7}{3}, \frac{71}{31}, \frac{1216}{531}.$$

Zwischen

$$\frac{1}{0} \text{ und } \frac{7}{3}, \frac{7}{3} \text{ und } \frac{71}{31}, \frac{71}{31} \text{ und } \frac{1216}{531}$$

liegen beziehungsweise die unvollständigen Quotienten 3, 4, 5. In das erste Intervall lassen sich also zwei Brüche einschalten, nämlich die Werte, welche der Ausdruck

$$\frac{2k+1}{k} \text{ für } k = 1, 2$$

annimmt, d. i.

$$\frac{3}{1} \text{ und } \frac{5}{2}.$$

In das zweite Intervall kommen drei Brüche, nämlich die Werte, welche der Ausdruck

$$\frac{16k+7}{7k+3} \text{ für } k = 1, 2, 3$$

annimmt, d. i.

$$\frac{23}{10}, \frac{39}{17}, \frac{55}{24}.$$

In das dritte Intervall kommen vier Brüche, nämlich die Werte, welche der Ausdruck

$$\frac{229k + 71}{100k + 31} \text{ für } k = 1, 2, 3, 4$$

annimmt, d. i.

$$\frac{300}{131}, \frac{529}{231}, \frac{758}{331}, \frac{987}{431}.$$

Die fallende Reihe wird somit

$$\left(\frac{1}{0}\right), \frac{3}{1}, \frac{5}{2}, \left(\frac{7}{3}\right), \frac{23}{10}, \frac{39}{17}, \frac{55}{24}, \left(\frac{71}{31}\right), \frac{300}{131}, \frac{529}{231}, \frac{758}{331}, \frac{987}{431}, \left(\frac{1216}{531}\right);$$

darin sind die ursprünglichen Näherungsbrüche zum Unterschiede von den eingeschalteten in Klammern gesetzt. Ebenso geht

B. die steigende Reihe

$$\frac{2}{1}, \frac{16}{7}, \frac{229}{100}$$

über in

$$\left(\frac{2}{1}\right), \frac{9}{4}, \left(\frac{16}{7}\right), \frac{87}{38}, \frac{158}{69}, \left(\frac{229}{100}\right).$$

II. Beispiel.

$$\frac{5096}{1595} = (3, 5, 7, 1, 3, 2, 4).$$

Die beiden Reihen werden

$$\text{A. (fallend): } \left(\frac{1}{0}\right), \frac{4}{1}, \frac{7}{2}, \frac{10}{3}, \frac{13}{4}, \left(\frac{16}{5}\right), \left(\frac{131}{41}\right), \frac{639}{200}, \left(\frac{1147}{359}\right).$$

$$\text{B. (steigend): } \left(\frac{3}{1}\right), \frac{19}{6}, \frac{35}{11}, \frac{51}{16}, \frac{67}{21}, \frac{83}{26}, \frac{99}{31}, \left(\frac{115}{36}\right), \frac{246}{77}, \frac{377}{118}, \\ \left(\frac{508}{159}\right), \frac{1655}{518}, \frac{2802}{877}, \frac{3949}{1236}, \left(\frac{5096}{1595}\right).$$

Es sei

$$\frac{P}{Q} = (\alpha, \alpha_1, \alpha_2, \dots, \alpha_{n-1}),$$

so ist nach §. 56

$$\frac{Q}{Q_{n-1}} = (\alpha_{n-1}, \alpha_{n-2}, \dots, \alpha_2, \alpha_1),$$

d. h. wenn man den ersten unvollständigen Quotienten eines Kettenbruchs weglässt und die übrigen in umgekehrter Reihenfolge nimmt, so ist der entstandene Kettenbruch gleich dem Nenner des letzten, dividiert durch den Nenner des vorletzten Näherungsbruchs des ursprünglichen Kettenbruchs.

Beispiel.

$$\frac{43}{19} = (2, 3, 1, 4).$$

Näherungsbrüche:

2	3	1	4	
$\frac{1}{0}$	$\frac{2}{1}$	$\frac{7}{3}$	$\frac{9}{4}$	$\frac{43}{19}$

$$\frac{43}{9} = (4, 1, 3, 2),$$

$$\frac{19}{4} = (4, 1, 3).$$

§. 60.

Symmetrische Kettenbrüche.

Ein Kettenbruch heißt symmetrisch, wenn in der Reihe der unvollständigen Quotienten die von den Enden gleich weit entfernten Glieder einander gleich sind. Es sind also

$$(\alpha, \alpha_1, \dots, \alpha_{k-1}, \alpha_k, \alpha_k, \alpha_{k-1}, \dots, \alpha_1, \alpha),$$

$$(\alpha, \alpha_1, \dots, \alpha_{k-1}, \alpha_k, \alpha_{k-1}, \dots, \alpha_1, \alpha)$$

symmetrische Kettenbrüche; der erstere enthält $2k + 2$, der letztere $2k + 1$ unvollständige Quotienten; beim ersten ist jeder Quotient zweimal vorhanden, beim zweiten der mittlere Quotient (α_k) nur einmal.

Beispiele:

$$\frac{2785}{1232} = (2, 3, 1, 5, 5, 1, 3, 2),$$

$$\frac{531}{235} = (2, 3, 1, 5, 1, 3, 2).$$

Lehrsatz I. Wenn ein rationaler Bruch $\frac{P}{Q}$, der größer als die Einheit ist, sich in einen symmetrischen Kettenbruch verwandeln läßt, so ist $Q^2 + 1$ oder $Q^2 - 1$ durch P teilbar, je nachdem die Anzahl der unvollständigen Quotienten gerade oder ungerade ist.

Beweis. Es sei

$$\frac{P}{Q} = (\alpha, \alpha_1, \alpha_2, \dots, \alpha_{n-1}),$$

so ist nach §. 59

$$\frac{P}{P_{n-1}} = (\alpha_{n-1}, \alpha_{n-2}, \dots, \alpha_1, \alpha),$$

und da beide Kettenbrüche identisch sein sollen, so muß

$$\frac{P}{Q} = \frac{P}{P_{n-1}}, \text{ also } Q = P_{n-1}$$

sein. Für diesen Wert von P_{n-1} geht die Formel

$$P Q_{n-1} - P_{n-1} Q = (-1)^n$$

des §. 57 über in

$$P Q_{n-1} - Q^2 = (-1)^n.$$

Es ist also

$$Q_{n-1} = \frac{Q^2 + (-1)^n}{P},$$

und da Q_{n-1} eine ganze Zahl ist, so muß P in $Q^2 + (-1)^n$ aufgehen, d. h. es ist $Q^2 + 1$ oder $Q^2 - 1$ durch P teilbar, je nachdem n gerade oder ungerade ist.

Beispiele (siehe oben):

$$1232^2 + 1 = 1517825 = 545 \cdot 2785,$$

$$235^2 - 1 = 55224 = 14 \cdot 531.$$

Lehrsatz II. (Umkehrung). Wenn $Q^2 \pm 1$ durch P teilbar ist, so liefert die Entwicklung von $\frac{P}{Q}$ einen symmetrischen Kettenbruch.

Beweis. Da man den letzten unvollständigen Quotienten α_{n-1} eines Kettenbruchs nötigen Falls durch

$$(\alpha_{n-1} - 1) + \frac{1}{1}$$

ersetzen kann, so sind wir imstande, die Anzahl der Quotienten nach Belieben zu einer geraden oder ungeraden zu machen. Wir entwickeln nun $\frac{P}{Q}$ in einen Kettenbruch, dessen Quotientenzahl n gerade oder ungerade ist, je nachdem P in $Q^2 + 1$ oder in $Q^2 - 1$ aufgeht; dann ist

$$\frac{Q^2 + (-1)^n}{P}$$

eine ganze Zahl, die wir R nennen wollen, also

$$RP = Q^2 + (-1)^n.$$

Ferner ist, wenn $\frac{P_{n-1}}{Q_{n-1}}$ den vorletzten Näherungsbruch bezeichnet,

$$PQ_{n-1} - P_{n-1}Q = (-1)^n,$$

und aus diesen beiden Gleichungen folgt

$$P(R - Q_{n-1}) = Q(Q - P_{n-1}).$$

Die linke Seite dieser Gleichung ist durch P teilbar, folglich muß es auch die rechte sein, und da Q prim zu P ist, so muß P in $Q - P_{n-1}$ aufgehen. Diese Differenz ist aber kleiner als P ; sie ist daher gleich Null, d. h. es ist $Q = P_{n-1}$. Dann ist aber der Kettenbruch, den die Entwicklung von $\frac{P}{Q}$ liefert, mit demjenigen, welcher $\frac{P}{P_{n-1}}$ darstellt, d. i. mit seiner Umkehrung, identisch; er ist folglich symmetrisch.

§. 61.

Zerfällung von Zahlen in zwei Quadrate.

Lehrsatz I. Wenn die Näherungsbrüche des symmetrischen Kettenbruchs von gerader Quotientenzahl

$$(\alpha, \alpha_1, \dots, \alpha_{n-1}, \alpha_{n-1}, \dots, \alpha_1, \alpha)$$

mit

$$\frac{P_0}{Q_0}, \frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \dots, \frac{P_{2n-1}}{Q_{2n-1}}, \frac{P_{2n}}{Q_{2n}}$$

bezeichnet werden, so ist

$$P_{2n} = P_n^2 + P_{n-1}^2 \quad \text{und} \quad Q_{2n-1} = Q_n^2 + Q_{n-1}^2.$$

Beweis. Es ist

$$\frac{P_n}{Q_n} = (\alpha, \alpha_1, \dots, \alpha_{n-2}, \alpha_{n-1})$$

und nach §. 59

$$\frac{P_n}{P_{n-1}} = (\alpha_{n-1}, \alpha_{n-2}, \dots, \alpha_1, \alpha),$$

also

$$\frac{P_{n-1}}{P_n} = (0, \alpha_{n-1}, \alpha_{n-2}, \dots, \alpha_1, \alpha).$$

Nun verwandelt sich

$$\frac{P_n}{Q_n} \quad \text{in} \quad \frac{P_{2n}}{Q_{2n}},$$

wenn man α_{n-1} durch

$$(\alpha_{n-1}, \alpha_{n-1}, \alpha_{n-2}, \dots, \alpha_1, \alpha),$$

d. i. durch

$$\alpha_{n-1} + \frac{P_{n-1}}{P_n}$$

ersetzt. Die Formel

$$\frac{P_n}{Q_n} = \frac{P_{n-1} \alpha_{n-1} + P_{n-2}}{Q_{n-1} \alpha_{n-1} + Q_{n-2}}$$

liefert also

$$\begin{aligned} \frac{P_{2n}}{Q_{2n}} &= \frac{P_{n-1} \left(\alpha_{n-1} + \frac{P_{n-1}}{P_n} \right) + P_{n-2}}{Q_{n-1} \left(\alpha_{n-1} + \frac{P_{n-1}}{P_n} \right) + Q_{n-2}} \\ &= \frac{P_{n-1}^2 + P_n (P_{n-1} \alpha_{n-1} + P_{n-2})}{P_n (Q_{n-1} \alpha_{n-1} + Q_{n-2}) + P_{n-1} Q_{n-1}}, \end{aligned}$$

und daher ist nach §. 56

$$(1) \quad \frac{P_{2n}}{Q_{2n}} = \frac{P_n^2 + P_{n-1}^2}{P_n Q_n + P_{n-1} Q_{n-1}}.$$

Ebenso ist weiter nach §. 59

$$\frac{Q_n}{Q_{n-1}} = (\alpha_{n-1}, \alpha_{n-2}, \dots, \alpha_2, \alpha_1),$$

folglich

$$\frac{Q_{n-1}}{Q_n} = (0, \alpha_{n-1}, \alpha_{n-2}, \dots, \alpha_2, \alpha_1),$$

und da sich

$$\frac{P_n}{Q_n} \text{ in } \frac{P_{2n-1}}{Q_{2n-1}}$$

verwandelt, wenn man α_{n-1} durch

$$(\alpha_{n-1}, \alpha_{n-1}, \alpha_{n-2}, \dots, \alpha_2, \alpha_1),$$

d. i. durch

$$\alpha_{n-1} + \frac{Q_{n-1}}{Q_n}$$

ersetzt, so erhalten wir

$$\begin{aligned} \frac{P_{2n-1}}{Q_{2n-1}} &= \frac{P_{n-1} \left(\alpha_{n-1} + \frac{Q_{n-1}}{Q_n} \right) + P_{n-2}}{Q_{n-1} \left(\alpha_{n-1} + \frac{Q_{n-1}}{Q_n} \right) + Q_{n-2}} \\ &= \frac{Q_n (P_{n-1} \alpha_{n-1} + P_{n-2}) + P_{n-1} Q_{n-1}}{Q_n (Q_{n-1} \alpha_{n-1} + Q_{n-2}) + Q_{n-1}^2}. \end{aligned}$$

Es ist also nach §. 56

$$(2) \quad \frac{P_{2n-1}}{Q_{2n-1}} = \frac{P_n Q_n + P_{n-1} Q_{n-1}}{Q_n^2 + Q_{n-1}^2}.$$

Die linken Seiten der Formeln (1) und (2) sind irreduzibele Brüche; was die rechten betrifft, so ist

$$\begin{aligned} P_n (P_n Q_n + P_{n-1} Q_{n-1}) - Q_n (P_n^2 + P_{n-1}^2) &= \\ P_{n-1} (P_n Q_{n-1} - P_{n-1} Q_n) &= (-1)^n P_{n-1} \end{aligned}$$

und

$$\begin{aligned} P_n (Q_n^2 + Q_{n-1}^2) - Q_n (P_n Q_n + P_{n-1} Q_{n-1}) &= \\ Q_{n-1} (P_n Q_{n-1} - P_{n-1} Q_n) &= (-1)^n Q_{n-1}. \end{aligned}$$

Ein gemeinschaftlicher Divisor des Zählers und des Nenners der rechten Seite von (1) müßte also auch in P_{n-1} aufgehen; derselbe wäre demnach ein gemeinschaftlicher Divisor von P_n und P_{n-1} , während nach §. 57 der Bruch $\frac{P_n}{P_{n-1}}$ irreduzibel ist. Somit ist auch die rechte Seite von (1) irreduzibel. Da ferner ein gemeinschaftlicher Divisor des Zählers und des Nenners der rechten Seite von (2) in Q_{n-1} , also auch in Q_n aufgehen müßte, während doch $\frac{Q_n}{Q_{n-1}}$ ein irreduzibeler Bruch ist, so muß auch die

rechte Seite von (2) irreduzibel sein. Es ist somit

$$P_{2n} = P_n^2 + P_{n-1}^2, \quad Q_{2n-1} = Q_n^2 + Q_{n-1}^2.$$

Beispiel:

$$\frac{2785}{1232} = (2, 3, 1, 5, 5, 1, 3, 2).$$

Näherungsbrüche:

2	3	1	5	5	1	3	2	
$\frac{1}{0}$	$\frac{2}{1}$	$\frac{7}{3}$	$\frac{9}{4}$	$\frac{52}{23}$	$\frac{269}{119}$	$\frac{321}{142}$	$\frac{1232}{545}$	$\frac{2785}{1232}$

$$2785 = 52^2 + 9^2, \quad 545 = 23^2 + 4^2.$$

Lehrsatz II. Wenn eine ganze Zahl N in die Summe zweier Quadrate aufgeht, die prim zu einander sind, so ist sie selbst die Summe zweier Quadrate.

Beweis. Die Zahl N soll in $R^2 + S^2$ aufgehen, wo $R > S$ und prim zu S vorausgesetzt wird. Wenn wir dann $\frac{R}{S}$ in einen Kettenbruch entwickeln und den vorletzten Näherungsbruch desselben $\frac{r}{s}$ nennen, so ist

$$Rs - rS = \pm 1.$$

Da nun N in $R^2 + S^2$ aufgeht, so muß auch

$$(R^2 + S^2)(r^2 + s^2) = (Rr + Ss)^2 + (Rs - rS)^2 = (Rr + Ss)^2 + 1$$

durch N teilbar sein. N geht dann auch in

$$(Rr + Ss - kN)^2 + 1$$

auf, wo k jede ganze Zahl sein kann.

Wir verfügen jetzt über k so, daß

$$Rr + Ss - kN < N$$

werde; dann haben wir eine Zahl $Rr + Ss - kN$, die der Kürze wegen Q genannt werden möge, die kleiner als N und so beschaffen ist, daß N in $Q^2 + 1$ aufgeht.

Wenn wir daher $\frac{N}{Q}$ in einen Kettenbruch von gerader Quotientenzahl entwickeln, so wird derselbe symmetrisch sein.

Nehmen wir

$$\frac{N}{Q} = (\alpha, \alpha_1, \dots, \alpha_{n-1}, \alpha_{n-1}, \dots, \alpha_1, \alpha)$$

an, so ist nach dem vorigen Satze

$$P_{2n} \text{ d. i. } N = P_n^2 + P_{n-1}^2.$$

Zusatz. Jede Primzahl von der Form $4n + 1$ läßt sich in zwei Quadrate zerfällen.

Beweis. Nach dem Zusatz zum Wilsonschen Satze (§. 43) ist, wenn $p = 4n + 1$ ist, $(1 \cdot 2 \cdot 3 \dots 2n)^2 + 1$ durch p teilbar; folglich ist in diesem Falle p die Summe zweier Quadrate.

Aufgabe I. Die Summe zweier Quadrate, die prim zu einander sind, zu finden, ohne die Quadrate selbst zu berechnen.

Lösung. Es soll $a^2 + b^2$, wo $a > b$ und prim zu b ist, berechnet werden. Man entwickle $\frac{a}{b}$ in einen Kettenbruch. Wenn

$$\frac{a}{b} = (\alpha, \alpha_1, \dots, \alpha_{n-1})$$

und $\frac{P_{2n}}{Q_{2n}}$ der Wert des symmetrischen Kettenbruchs

$$(\alpha_{n-1}, \alpha_{n-2}, \dots, \alpha_1, \alpha, \alpha, \alpha_1, \dots, \alpha_{n-1})$$

ist, so hat man

$$a^2 + b^2 = P_{2n}.$$

Beispiel. Es soll die Summe $19^2 + 48^2$ bestimmt werden.

$$\frac{48}{19} = (2, 1, 1, 9).$$

9	1	1	2	2	1	1	9
1	9	10	19	48	115	163	278
							2665.

Es ist somit $19^2 + 48^2 = 2665$.

Aufgabe II. Eine Zahl N , die in der Summe $R^2 + S^2$ aufgeht, wo $R > S$ und prim zu S ist, in zwei Quadrate zu zerfällen.

Lösung. Man entwickle $\frac{R}{S}$ in einen Kettenbruch, nehme den vorletzten Näherungsbruch $\frac{r}{s}$ desselben und bilde die Zahl $Rr + Ss$.

Der kleinste positive Rest dieser Zahl für den Modul N sei Q ; dann geht N in $Q^2 + 1$ auf. Wenn wir also $\frac{N}{Q}$ in einen Kettenbruch entwickeln, so wird derselbe symmetrisch sein und eine gerade Anzahl Quotienten enthalten. Es sei

$$\frac{N}{Q} = (\alpha, \alpha_1, \dots, \alpha_{n-1}, \alpha_{n-1}, \dots, \alpha_1, \alpha);$$

dann ist

$$N = P_n^2 + P_{n-1}^2.$$

Beispiel.

$$13^2 + 124^2 = 5 \cdot 3109.$$

$$\frac{124}{13} = (9, 1, 1, 6).$$

9	1	1	6	
$\frac{1}{0}$	$\frac{9}{1}$	$\frac{10}{1}$	$\frac{19}{2}$	$\frac{124}{13}$

$$Q = 124 \cdot 19 + 13 \cdot 2 = 2382.$$

$$\frac{3109}{2382} = (1, 3, 3, 1, 1, 1, 1, 1, 1, 3, 3, 1).$$

1	3	3	1	1	1	
1	1	4	13	17	30	47.

$$3109 = 47^2 + 30^2.$$

Aufgabe III. Die Primzahl $p = 4n + 1$ in zwei Quadrate zu zerfallen.

Lösung. Man ermittle eine Wurzel der Kongruenz

$$x^2 \equiv -1 \pmod{p},$$

deren Lösung uns in §. 79 und 121 beschäftigen wird. Ist q eine solche Wurzel, so ist $q^2 + 1$ durch p teilbar, die Aufgabe also auf die vorhergehende zurückgeführt.

Beispiel. Es soll 1973 in zwei Quadrate zerfällt werden. Die Kongruenz

$$x^2 \equiv -1 \pmod{1973}$$

hat die Wurzeln ± 259 . Weiter ist

$$\frac{1973}{259} = (7, 1, 1, 1, 1, 1, 1, 1, 7),$$

7	1	1	1	1	
1	7	8	15	23	38,

$$1973 = 38^2 + 23^2.$$

Aufgabe IV. Mittels der Zerfällung

$$p = a^2 + b^2,$$

wo $a > b$ (und prim zu b) ist, eine Wurzel der Kongruenz

$$x^2 \equiv -1 \pmod{p}$$

zu finden.

1. Lösung. Man entwickle $\frac{a}{b}$ in einen Kettenbruch und bilde dessen Näherungsbrüche. Wenn der vorletzte derselben $\frac{a'}{b'}$ ist, so ist nach den im Beweise des Lehrsatzes II gegebenen Entwicklungen $(aa' + bb')^2 + 1$ durch p teilbar, also $aa' + bb'$ eine Wurzel der Kongruenz $x^2 \equiv -1 \pmod{p}$ [Euler, Commentationes arithm. coll. I, S. 359].

2. Lösung. Man entwickle $\frac{a}{b}$ in einen Kettenbruch,

$$\frac{a}{b} = (\alpha_{n-1}, \dots, \alpha_1, \alpha),$$

und berechne die Zähler der Näherungsbrüche des symmetrischen Kettenbruchs

$$(\alpha, \alpha_1, \dots, \alpha_{n-1}, \alpha_{n-1}, \dots, \alpha_1, \alpha).$$

Der vorletzte dieser Zähler ist eine Wurzel der Kongruenz

$$x^2 \equiv -1 \pmod{p}.$$

Beispiel. Mittels der Zerfällung

$$433 = 17^2 + 12^2$$

die Kongruenz

$$x^2 \equiv -1 \pmod{433}$$

zu lösen.

1. Lösung.

$$\frac{17}{12} = (1, 2, 2, 2).$$

1	2	2	2	
$\frac{1}{0}$	$\frac{1}{1}$	$\frac{8}{2}$	$\frac{7}{5}$	$\frac{17}{12}$

$$x = 7 \cdot 17 + 5 \cdot 12 = 179.$$

2. Lösung.

2	2	2	1	1	2	2	2	
1	2	5	12	17	29	75	179	433,

$$x = 179.$$

Anmerkung. Euler giebt l. c. S. 362 ff. für die unter 2000 liegenden Primzahlen $p = 4n + 1$ die Zerfällung in zwei Quadrate und die Wurzeln der Kongruenz

$$x^2 \equiv -1 \pmod{p}.$$

§. 62.

Auflösung der Kongruenz ersten Grades mit einer Unbekannten (Lagrange, Oeuvres II, S. 696 u. VII, S. 89).

Um die Kongruenz

$$ax \equiv b \pmod{m},$$

d. i. die unbestimmte Gleichung

$$ax - my = b$$

zu lösen, entwickeln wir $\frac{a}{m}$ in einen Kettenbruch von gerader oder ungerader Quotientenzahl, je nachdem b eine positive oder negative Zahl ist. Der letzte Näherungsbruch des Kettenbruchs ist $\frac{a}{m}$, der vorletzte sei $\frac{\alpha}{\mu}$; dann ist

$$a\mu - \alpha m = \pm 1,$$

und zwar hat hier die rechte Seite dasselbe Vorzeichen wie die Zahl b in der vorgelegten Kongruenz. Es ergibt sich also durch Multiplikation mit dem absoluten Werte von b

$$a\mu[b] - \alpha m[b] = b;$$

somit ist

$$x = \mu[b], \quad y = \alpha[b]$$

eine Lösung der unbestimmten Gleichung und

$$x \equiv \mu[b] \pmod{m}$$

die Lösung der vorgelegten Kongruenz.

Anmerkung. Mit diesem Verfahren stimmt im wesentlichen die Zerstäubungsmethode der Inder überein. Siehe Colebrooke, S. 156. Vergl. auch Cantor, Vorlesungen über Geschichte der Mathematik, Bd. I, S. 588 ff.

Beispiele:

I. $7x \equiv +2 \pmod{11}.$

$$\frac{7}{11} = (0, 1, 1, 1, 2, 1).$$

0	1	1	1	2	1	
$\frac{1}{0}$	$\frac{0}{1}$	$\frac{1}{1}$	$\frac{1}{2}$	$\frac{2}{3}$	$\frac{5}{8}$	$\frac{7}{11}$

$$7 \cdot 8 - 11 \cdot 5 = +1,$$

$$7 \cdot 16 - 11 \cdot 10 = +2,$$

$$x \equiv 16 \equiv 5 \pmod{11}.$$

II. $7x \equiv -2 \pmod{11}.$

$$\frac{7}{11} = (0, 1, 1, 1, 3).$$

0	1	1	1	3	
$\frac{1}{0}$	$\frac{0}{1}$	$\frac{1}{1}$	$\frac{1}{2}$	$\frac{2}{3}$	$\frac{7}{11}$

$$7 \cdot 3 - 11 \cdot 2 = -1,$$

$$7 \cdot 6 - 11 \cdot 4 = -2,$$

$$x \equiv 6 \pmod{11}.$$

III. Wenn man das Fünffache einer Zahl durch 63 dividiert, so erhält man den Rest 7. Welche Zahl ist es? (Bhāscara, Colebrooke, S. 169.)

$$5x \equiv 7 \pmod{63},$$

$$\frac{5}{63} = (0, 12, 1, 1, 1, 1).$$

0	12	1	1	1	1	
$\frac{1}{0}$	$\frac{0}{1}$	$\frac{1}{12}$	$\frac{1}{18}$	$\frac{2}{25}$	$\frac{3}{38}$	$\frac{5}{63}$

$$5 \cdot 38 - 63 \cdot 3 = 1,$$

$$5 \cdot (38 \cdot 7) - 63 \cdot (3 \cdot 7) = 7,$$

$$x \equiv 266 \equiv 14 \pmod{63}.$$

§. 63.

Irrationale Größen, deren Entwicklungen in Kettenbrüche zu einem und demselben vollständigen Quotienten führen.

Lehrsatz I. Wenn die Entwicklungen zweier irrationalen Größen x, x' in Kettenbrüche zu demselben vollständigen Quotienten y führen, so besteht die Gleichung

$$x' = \frac{ax + b}{cx + d},$$

wo a, b, c, d ganze Zahlen sind, die der Bedingung

$$ad - bc = \pm 1$$

genügen.

Beweis. Wir nehmen an, es sei

$$x = \left(\alpha, \alpha_1, \alpha_2, \dots, \alpha_{k-1} + \frac{1}{y} \right),$$

$$x' = \left(\alpha', \alpha'_1, \alpha'_2, \dots, \alpha'_{m-1} + \frac{1}{y} \right),$$

und bezeichnen die Näherungsbrüche von x mit $\frac{P}{Q}$, diejenigen

von x' mit $\frac{P'}{Q'}$, dann ist

$$x = \frac{P_k y + P_{k-1}}{Q_k y + Q_{k-1}}, \quad \text{folglich} \quad y = \frac{P_{k-1} - Q_{k-1} x}{Q_k x - P_k},$$

$$x' = \frac{P'_m y + P'_{m-1}}{Q'_m y + Q'_{m-1}}, \quad \text{folglich} \quad y = \frac{P'_{m-1} - Q'_{m-1} x'}{Q'_m x' - P'_m}.$$

Durch Gleichsetzung beider Werte von y und leichte Vereinfachungen ergibt sich dann

$$x' = \frac{(P'_m Q_{k-1} - P'_{m-1} Q_k) x + (P_k P'_{m-1} - P_{k-1} P'_m)}{(Q_{k-1} Q'_m - Q_k Q'_{m-1}) x + (P'_k Q'_{m-1} - P_{k-1} Q'_m)},$$

oder, wenn

$$P'_m Q_{k-1} - P'_{m-1} Q_k = a,$$

$$P_k P'_{m-1} - P_{k-1} P'_m = b,$$

$$Q_{k-1} Q'_m - Q_k Q'_{m-1} = c,$$

$$P'_k Q'_{m-1} - P_{k-1} Q'_m = d$$

gesetzt wird,

$$x' = \frac{a x + b}{c x + d}.$$

Weiter erhält man durch wirkliche Ausrechnung

$$ad - bc = (P_k Q_{k-1} - P_{k-1} Q_k)(P'_m Q'_{m-1} - P'_{m-1} Q'_m) = (-1)^k (-1)^m = \pm 1.$$

Lehrsatz II. (Umkehrung.) Wenn zwei irrationale Größen x, x' der Gleichung

$$x' = \frac{a x + b}{c x + d}$$

genügen, wo a, b, c, d ganze Zahlen sind, für welche

$$ad - bc = \pm 1$$

ist, so haben die Kettenbrüche, in welche sich x und x' entwickeln lassen, einen vollständigen Quotienten y gemeinschaftlich.

Beweis. Es sei wieder

$$x = \left(\alpha, \alpha_1, \alpha_2, \dots, \alpha_{k-1} + \frac{1}{y} \right),$$

also

$$x = \frac{P_k y + P_{k-1}}{Q_k y + Q_{k-1}};$$

dann ergibt sich

$$x' = \frac{(a P_k + b Q_k)y + (a P_{k-1} + b Q_{k-1})}{(c P_k + d Q_k)y + (c P_{k-1} + d Q_{k-1})},$$

oder, wenn

$$\begin{aligned} a P_k + b Q_k &= A, & a P_{k-1} + b Q_{k-1} &= B, \\ c P_k + d Q_k &= C, & c P_{k-1} + d Q_{k-1} &= D \end{aligned}$$

gesetzt wird,

$$x' = \frac{A y + B}{C y + D},$$

und es ist

$$A D - B C = (a d - b c)(P_k Q_{k-1} - P_{k-1} Q_k) = \pm 1.$$

Entwickelt man jetzt $\frac{A}{C}$ in einen Kettenbruch und bezeichnet den vorletzten Näherungsbruch desselben mit $\frac{B'}{D'}$, so ist

$$A D' - B' C = \pm 1,$$

und da wir die Anzahl der Quotienten des Kettenbruchs nach Belieben gerade oder ungerade machen können, so dürfen wir

$$A D - B C = A D' - B' C$$

voraussetzen. Daraus folgt

$$A(D - D') = C(B - B').$$

Nun erkennt man leicht, daß A prim zu C ist; ein gemeinschaftlicher Divisor beider Zahlen müßte nämlich wegen der Gleichung

$$A D - B C = \pm 1$$

auch in 1 aufgehen. Weiter lehren die Formeln, welche A, B, C, D definieren, daß $A > B$, also umsomehr $A > B'$ ist. A kann also in $C(B - B')$ nur aufgehen, wenn $B - B' = 0$ ist. Es ist somit $B = B'$; ebenso ist $D = D'$, also

$$x' = \frac{A y + B'}{C y + D'},$$

d. h. y ist ein vollständiger Quotient von x' wie von x .

§. 64.

Periodische Kettenbrüche.

Ein unendlicher Kettenbruch heißt periodisch, wenn die vollständigen, also auch die unvollständigen Quotienten von einer Stelle

an in unveränderter Folge wiederkehren. Die sich in dieser Weise wiederholenden Quotienten bilden die Periode des Kettenbruchs. Die Periode kann ein- und mehrgliedrig sein. Wenn dieselbe gleich mit dem ersten Quotienten beginnt, so heißt der Kettenbruch rein periodisch; wenn ein oder mehrere Glieder der Periode vorangehen, so wird der Kettenbruch unrein periodisch genannt. Wir werden in der Folge die Periode durch einen darüber gesetzten Strich kenntlich machen.

Beispiele. I. Der Kettenbruch

$$x = (\overline{1, 2}, 1, 2, \dots)$$

ist rein periodisch; die Periode besteht aus zwei Quotienten. Um einen geschlossenen Ausdruck für x zu erhalten, beachten wir, daß

$$x = 1 + \frac{1}{2} + \frac{1}{x}$$

ist, bilden also die Näherungsbrüche des Kettenbruchs $(1, 2, x)$. Es ergibt sich

1	2	x	
$\frac{1}{0}$	$\frac{1}{1}$	$\frac{3}{2}$	$\frac{3x+1}{2x+1}$

Somit ist

$$x = \frac{3x+1}{2x+1},$$

d. h. x ist eine Wurzel der Gleichung

$$2x^2 - 2x = 1.$$

II. Der Kettenbruch

$$x = (3, \overline{7, 4}, 7, \dots)$$

ist unrein periodisch, da der Periode $7, 4$ der Quotient 3 vorangeht. Man erhält

$$x - 3 = \frac{1}{7} + \frac{1}{4 + x - 3} = \frac{1}{7} + \frac{1}{x + 1},$$

0	7	$x + 1$	
$\frac{1}{0}$	$\frac{0}{1}$	$\frac{1}{7}$	$\frac{x + 1}{7x + 8}$

Also besteht die Gleichung

$$x - 3 = \frac{x + 1}{7x + 8},$$

und somit ist x eine Wurzel der Gleichung

$$7x^2 - 14x = 25.$$

III. Wenn

$$x = (3, \overline{1, 6}, 1, \dots)$$

ist, so ergibt sich der Reihe nach

$$x - 3 = \frac{1}{1} + \frac{1}{6 + x - 3} = (0, 1, x + 3),$$

0	1	$x + 3$	
$\frac{1}{0}$	$\frac{0}{1}$	$\frac{1}{1}$	$\frac{x + 3}{x + 4}$

$$x - 3 = \frac{x + 3}{x + 4}.$$

$$x^2 = 15,$$

$$x = \sqrt{15}.$$

§. 65.

Verwandlung der irrationalen Wurzeln gemischt quadratischer Gleichungen in Kettenbrüche.

Zum besseren Verständnis der allgemeinen Entwicklung schicken wir ein Beispiel voraus.

Die Gleichung $3x^2 - 7x = 15$ hat die Wurzeln

$$x = \frac{7 \pm \sqrt{229}}{6}.$$

Es soll zunächst

$$x = \frac{7 + \sqrt{229}}{6}$$

in einen Kettenbruch entwickelt werden. Da 15 die Quadratwurzel der größten unter 229 liegenden Quadratzahl, folglich 3 die größte in $\frac{7 + \sqrt{229}}{6}$ enthaltene ganze Zahl ist, so setzen wir

$$x = \frac{7 + \sqrt{229}}{6} = 3 + \frac{-11 + \sqrt{229}}{6} = 3 + \frac{1}{x_1};$$

dann ist

$$x_1 = \frac{6}{-11 + \sqrt{229}} = \frac{6(11 + \sqrt{229})}{108} = \frac{11 + \sqrt{229}}{18}.$$

Weiter ist 1 die größte in

$$\frac{11 + \sqrt{229}}{18} = x_1$$

enthaltene ganze Zahl. Wir setzen daher

$$x_1 = 1 + \frac{-7 + \sqrt{229}}{18} = 1 + \frac{1}{x_2}.$$

Ebenso ergibt sich weiter

$$\begin{aligned} x_2 &= \frac{18}{-7 + \sqrt{229}} = \frac{18(7 + \sqrt{229})}{180} = \frac{7 + \sqrt{229}}{10} \\ &= 2 + \frac{-13 + \sqrt{229}}{10} = 2 + \frac{1}{x_3}, \end{aligned}$$

$$\begin{aligned} x_3 &= \frac{10}{-13 + \sqrt{229}} = \frac{10(13 + \sqrt{229})}{60} = \frac{13 + \sqrt{229}}{6} \\ &= 4 + \frac{-11 + \sqrt{229}}{6} = 4 + \frac{1}{x_4}, \end{aligned}$$

$$x_4 = \frac{6}{-11 + \sqrt{229}}.$$

x_4 ist genau die Zahl, die oben mit x_1 bezeichnet worden ist, so daß wir für x den Kettenbruch

$$x = (3, \overline{1, 2, 4}, 1, \dots)$$

mit der Periode 1, 2, 4 erhalten.

Die zweite Wurzel x' der Gleichung ist negativ. Wir entwickeln $-x'$ in einen Kettenbruch und erhalten auf die dargestellte Weise

$$-x' = (1, \overline{2, 1, 4}, 2, \dots).$$

Für diese Wurzel ist die Periode 2, 1, 4; da wir aber auch

$$-x' = (1, 2, 1, 4, 2, 1, 4, \dots)$$

schreiben, d. h. die Periode mit dem vierten Quotienten beginnen können, so sehen wir, daß die Periode von $-x'$ sich als Umkehrung derjenigen von x ansehen läßt.

Ganz so gestaltet sich das Verfahren im allgemeinen Falle. Es sei

$$Ax^2 + 2Bx + C = 0$$

eine Gleichung zweiten Grades mit ganzen Koeffizienten, für welche $B^2 - AC = D$ positiv und keine Quadratzahl ist, so daß die Wurzeln der Gleichung

$$\frac{-B + \sqrt{D}}{A} \quad \text{und} \quad \frac{-B - \sqrt{D}}{A}$$

irrational sind. Wir stellen uns die Aufgabe, eine der Wurzeln,

etwa $\frac{-B + \sqrt{D}}{A}$, in einen Kettenbruch zu entwickeln. Wir

setzen diese Wurzel, die wir mit x bezeichnen wollen, als positiv voraus; sollte dieselbe einen negativen Wert haben, so würden wir $-x$ in einen Kettenbruch verwandeln.

Bezeichnet α die größte in

$$(1) \quad x = \frac{-B + \sqrt{D}}{A}$$

enthaltene Zahl, die auch gleich Null sein kann, so setzen wir

$$x = \alpha + \frac{1}{x_1};$$

dann ist $\frac{1}{x_1}$ ein positiver echter Bruch, folglich $x_1 > +1$. Da nun

$$\frac{-B + \sqrt{D}}{A} = \alpha + \frac{-A\alpha - B + \sqrt{D}}{A}$$

ist, so erhalten wir als Wert von x_1

$$x_1 = \frac{A}{-A\alpha - B + \sqrt{D}},$$

und hieraus ergibt sich durch Erweiterung mit $A\alpha + B + \sqrt{D}$ und leichte Vereinfachungen

$$x_1 = \frac{A\alpha + B + \sqrt{D}}{-(A\alpha^2 + 2B\alpha + C)}$$

oder, wenn der Kürze wegen

$$A\alpha + B = B_1, \quad -(A\alpha^2 + 2B\alpha + C) = A_1$$

gesetzt wird,

$$(2) \quad x_1 = \frac{B_1 + \sqrt{D}}{A_1}.$$

Da $x_1 > +1$ ist, so wird die größte in x_1 enthaltene ganze Zahl, die wir α_1 nennen wollen, von Null verschieden sein. Übrigens hat x_1 genau dieselbe Form wie x , kann also auf ganz dieselbe Weise behandelt werden. Es ergibt sich

$$x_1 = \alpha_1 + \frac{1}{x_2}$$

und

$$(3) \quad x_2 = \frac{B_2 + \sqrt{D}}{A_2},$$

wo B_2, A_2 ebenso wie B_1, A_1 ganze Zahlen bezeichnen. Da auch $x_2 > +1$ ist, so läßt sich das Verfahren fortsetzen. Wir erhalten auf diese Weise

$$x = (\alpha, \alpha_1, \alpha_2, \dots, \alpha_{k-1}, x_k),$$

wo $\alpha, \alpha_1, \dots, \alpha_{k-1}$ positive ganze Zahlen sind. α kann auch Null sein, während die übrigen Quotienten von Null verschieden sind. x_k ist $> +1$ und hat die Form

$$\frac{B_k + \sqrt{D}}{A_k},$$

wo B_k, A_k ganze Zahlen bezeichnen.

Wir wollen jetzt beweisen, daß B_k und A_k für alle über eine gewisse Grenze hinaus liegenden Werte von k positiv sein werden.

Ersetzt man in der Formel

$$x = \frac{P_k x_k + P_{k-1}}{Q_k x_k + Q_{k-1}}$$

x durch

$$-\frac{B + \sqrt{D}}{A}$$

und x_k durch

$$\frac{B_k + \sqrt{D}}{A_k},$$

so erhält man durch leichte Vereinfachungen

$$- B_k(B Q_k + A P_k) - A_k(B Q_{k-1} + A P_{k-1}) + D Q_k \\ + \sqrt{D} \{ (B_k Q_k + A_k Q_{k-1}) - (B Q_k + A P_k) \} = 0,$$

und daraus ergeben sich, wenn sowohl der rationale, als auch der irrationale Teil gleich Null gesetzt wird, die Gleichungen

$$(1) - B_k(B Q_k + A P_k) - A_k(B Q_{k-1} + A P_{k-1}) = - D Q_k, \\ (2) \quad B_k Q_k \quad \quad \quad + A_k Q_{k-1} = B Q_k + A P_k,$$

durch deren Auflösung für A_k und B_k man bei Anwendung der Formel

$$P_k Q_{k-1} - P_{k-1} Q_k = (-1)^k$$

die folgenden Gleichungen erhält:

$$(3) \quad (-1)^k A A_k = (B Q_k + A P_k)^2 - D Q_k^2, \\ (4) \quad (-1)^{k+1} A B_k = - (D - B^2) Q_k Q_{k-1} \\ \quad \quad \quad + A B (P_k Q_{k-1} + P_{k-1} Q_k) + A^2 P_k P_{k-1}.$$

Wird in (4) D durch $B^2 - AC$ ersetzt, so ergibt sich

$$(4^*) \quad (-1)^{k+1} B_k = C Q_k Q_{k-1} + B (P_k Q_{k-1} + P_{k-1} Q_k) \\ \quad \quad \quad + A P_k P_{k-1}.$$

Nun folgt aus (3)

$$A_k = \frac{(-1)^k}{A} [B Q_k + A P_k + Q_k \sqrt{D}] [B Q_k + A P_k - Q_k \sqrt{D}] \\ = \frac{(-1)^k Q_k^2}{A} \left[A \frac{P_k}{Q_k} + B + 2\sqrt{D} - \sqrt{D} \right] \left[A \frac{P_k}{Q_k} + B - \sqrt{D} \right] \\ = (-1)^k Q_k^2 \left[2\sqrt{D} + A \left(\frac{P_k}{Q_k} - \frac{-B + \sqrt{D}}{A} \right) \right] \cdot \\ \quad \quad \quad \left[\frac{P_k}{Q_k} - \frac{-B + \sqrt{D}}{A} \right] \\ = (-1)^k Q_k^2 \left[2\sqrt{D} + A \left(\frac{P_k}{Q_k} - x \right) \right] \left[\frac{P_k}{Q_k} - x \right].$$

Je nachdem k gerade oder ungerade ist, ist

$$\frac{P_k}{Q_k} - x$$

positiv oder negativ. In jedem Falle ist also

$$(-1)^k \left(\frac{P_k}{Q_k} - x \right)$$

positiv. Ebenso wird bei wachsendem k , da dann die Differenz

$$\frac{P_k}{Q_k} - x$$

abnimmt, der Faktor

$$2\sqrt{D} + A\left(\frac{P_k}{Q_k} - x\right)$$

sich der positiven Grenze $2\sqrt{D}$ nähern. Somit ist A_k für alle über eine gewisse Grenze hinaus liegenden Werte von k positiv.

Dafs auch B_k eine positive Zahl ist, geht aus der Formel (2) hervor. Diese liefert

$$\frac{A_k Q_{k-1}}{Q_k} = A \frac{P_k}{Q_k} + B - B_k,$$

und daraus erhält man, wenn man durch die Gleichung

$$A_k x_k = B_k + \sqrt{D}$$

dividiert,

$$\frac{Q_{k-1}}{Q_k x_k} = \frac{A \frac{P_k}{Q_k} + B - B_k}{\sqrt{D} + B_k}.$$

Nun ist

$$x = \frac{-B + \sqrt{D}}{A},$$

also

$$\sqrt{D} = Ax + B;$$

folglich nähert sich bei wachsendem k der Ausdruck

$$A \frac{P_k}{Q_k} + B$$

der Grenze $\sqrt{D}$, somit

$$\frac{Q_{k-1}}{Q_k x_k}$$

der Grenze

$$\frac{\sqrt{D} - B_k}{\sqrt{D} + B_k},$$

und da

$$\frac{Q_{k-1}}{Q_k x_k} < 1$$

ist, so muß auch

$$\frac{\sqrt{D} - B_k}{\sqrt{D} + B_k} < 1,$$

d. h. B_k positiv und $< \sqrt{D}$ sein.

§. 66.

Sätze über die Kettenbrüche, welche die irrationalen Wurzeln gemischt quadratischer Gleichungen darstellen.

Lehrsatz I. Der Kettenbruch, welcher eine irrationale Wurzel einer gemischt quadratischen Gleichung mit ganzen Koeffizienten darstellt, ist periodisch.

Beweis. Nach §. 65 ist die Zahl, die wir B_k genannt haben, kleiner als $< \sqrt{D}$. Da ferner

$$x_k = \frac{B_k + \sqrt{D}}{A_k} > 1$$

sein muß, so ist $A_k < B_k + \sqrt{D}$, also umsomehr $A_k < 2\sqrt{D}$. Es wird somit nach höchstens $\sqrt{D} \cdot 2\sqrt{D} = 2D$ Operationen ein vollständiger Quotient erscheinen, der schon da gewesen ist mit anderen Worten: der Kettenbruch ist periodisch.

Lehrsatz II. Jede Gröfse, die sich in einen periodischen Kettenbruch entwickeln läßt, ist Wurzel einer quadratischen Gleichung mit ganzen Koeffizienten.

Beweis. Es sei erstens

$$x = (\alpha, \alpha_1, \alpha_2, \dots, \alpha_{k-1}, \alpha, \dots),$$

der Kettenbruch also rein periodisch. Dann ist

$$x = (\alpha, \alpha_1, \alpha_2, \dots, \alpha_{k-1}, x),$$

und wenn wir die Näherungsbrüche dieses Kettenbruchs bilden:

α	α_1	$\dots$	α_{k-1}	x	
$\frac{1}{0}$	$\frac{\alpha}{1}$	$\dots$	$\frac{P_{k-1}}{Q_{k-1}}$	$\frac{P_k}{Q_k}$	$\frac{P_k x + P_{k-1}}{Q_k x + Q_{k-1}}$

so erhalten wir, da der letzte Näherungsbruch gleich x ist,

$$x = \frac{P_k x + P_{k-1}}{Q_k x + Q_{k-1}},$$

oder x ist Wurzel der quadratischen Gleichung

$$Q_k x^2 + (Q_{k-1} - P_k)x - P_{k-1} = 0.$$

Zweitens sei x ein unrein periodischer Kettenbruch

$$x = (\alpha', \alpha'_1, \dots, \alpha'_{m-1}, \overline{\alpha, \alpha_1, \dots, \alpha_{k-1}}, \alpha, \dots)$$

mit der Periode $\alpha, \alpha_1, \dots, \alpha_{k-1}$. Dann ist

$$x - \alpha' = (0, \alpha'_1, \dots, \alpha'_{m-1}, \overline{\alpha, \alpha_1, \dots, \alpha_{k-1}}, \alpha, \dots),$$

folglich

$$\frac{1}{x - \alpha'} = (\alpha'_1, \dots, \alpha'_{m-1}, \overline{\alpha, \alpha_1, \dots, \alpha_{k-1}}, \alpha, \dots).$$

Ebenso erhält man

$$\frac{1}{x - \alpha'} - \alpha'_1 = (0, \alpha'_2, \dots, \alpha'_{m-1}, \overline{\alpha, \dots, \alpha_{k-1}}, \alpha, \dots),$$

$$\frac{1}{\frac{1}{x - \alpha'} - \alpha'_1},$$

d. i.

$$\frac{x - \alpha'}{1 + \alpha' \alpha'_1 - \alpha'_1 x} = (\alpha'_2, \dots, \alpha'_{m-1}, \overline{\alpha, \dots, \alpha_{k-1}}, \alpha, \dots).$$

Weiter ergibt sich

$$\frac{x - \alpha'}{1 + \alpha' \alpha'_1 - \alpha'_1 x} - \alpha'_2 = (0, \alpha'_3, \dots, \alpha'_{m-1}, \overline{\alpha, \dots, \alpha_{k-1}}, \alpha, \dots),$$

also

$$\frac{1 + \alpha' \alpha'_1 - \alpha'_1 x}{-(\alpha' + \alpha'_2 + \alpha' \alpha'_1 \alpha'_2) + (1 + \alpha'_1 \alpha'_2) x} = (\alpha'_3, \dots, \alpha'_{m-1}, \overline{\alpha, \dots, \alpha_{k-1}}, \alpha, \dots).$$

So fortschließend erkennt man, daß

$$\frac{\varphi(x)}{\psi(x)} = (\alpha, \alpha_1, \dots, \alpha_{k-1}, \alpha, \dots)$$

sein wird, wo $\varphi(x)$, $\psi(x)$ Funktionen ersten Grades von x mit ganzen Koeffizienten sind. Die rechte Seite ist jetzt ein rein periodischer Kettenbruch, so daß wir nach dem ersten Fall verfahren können. Wir setzen

$$\frac{\varphi(x)}{\psi(x)} = (\alpha, \alpha_1, \dots, \alpha_{k-1}, \frac{\varphi(x)}{\psi(x)})$$

und bilden die Näherungsbrüche:

α	α_1	$\dots$	α_{k-1}	$\frac{\varphi(x)}{\psi(x)}$	
$\frac{1}{0}$	$\frac{\alpha}{1}$	$\dots$	$\frac{P_{k-1}}{Q_{k-1}}$	$\frac{P_k}{Q_k}$	$\frac{P_k \frac{\varphi(x)}{\psi(x)} + P_{k-1}}{Q_k \frac{\varphi(x)}{\psi(x)} + Q_{k-1}}$

Wir erhalten die Gleichung

$$\frac{\varphi(x)}{\psi(x)} = \frac{P_k \frac{\varphi(x)}{\psi(x)} + P_{k-1}}{Q_k \frac{\varphi(x)}{\psi(x)} + Q_{k-1}}$$

oder

$$\frac{\varphi(x)}{\psi(x)} = \frac{P_k \varphi(x) + P_{k-1} \psi(x)}{Q_k \varphi(x) + Q_{k-1} \psi(x)},$$

und diese ist offenbar vom zweiten Grade in x .

Beispiel:

$$x = (1, 2, \overline{1, 2, 3}, 1, \dots),$$

$$x - 1 = (0, 2, \overline{1, 2, 3}, 1, \dots),$$

$$\frac{1}{x-1} = (2, \overline{1, 2, 3}, 1, \dots),$$

$$\frac{1}{x-1} - 2,$$

d. i.

$$\frac{3-2x}{x-1} = (0, \overline{1, 2, 3}, 1, \dots),$$

$$\frac{x-1}{3-2x} = (\overline{1, 2, 3}, 1, \dots) = \left(1, 2, 3, \frac{x-1}{3-2x}\right).$$

1	2	3	$\frac{x-1}{3-2x}$	
$\frac{1}{0}$	$\frac{1}{1}$	$\frac{3}{2}$	$\frac{10}{7}$	$\frac{\frac{10x-10}{3-2x} + 3}{\frac{7x-7}{3-2x} + 2} = \frac{4x-1}{3x-1}$

$$\frac{x-1}{3-2x} = \frac{4x-1}{3x-1},$$

$$11x^2 - 18x + 4 = 0.$$

Eine Wurzel dieser Gleichung, nämlich

$$\frac{9 + \sqrt{37}}{11},$$

ist in der That, wie das in §. 65 dargelegte Verfahren zeigt, gleich dem Kettenbruch

$$(1, 2, \overline{1, 2, 3}, 1, \dots).$$

Lehrsatz III. Wenn man beide irrationalen Wurzeln einer quadratischen Gleichung in Kettenbrüche entwickelt, so ist die Periode des einen die Umkehrung der Periode des andern.

Beweis. Da wir ein negatives x durch $-x$ und ein x , dessen absoluter Betrag < 1 ist, durch $\frac{1}{x}$ ersetzen können, so dürfen wir von vornherein x als positiv und > 1 voraussetzen. Es sei nun zunächst

$$x = (\alpha, \alpha_1, \alpha_2, \dots, \alpha_{k-1}, \alpha, \dots)$$

ein rein periodischer Kettenbruch, so ist, wie wir soeben gesehen haben, x eine Wurzel der Gleichung

$$Q_k x^2 + (Q_{k-1} - P_k)x - P_{k-1} = 0.$$

Das Produkt der Wurzeln dieser Gleichung ist bekanntlich $-\frac{P_{k-1}}{Q_k}$, und da P_{k-1} und Q_k positiv sind, so muß das Produkt negativ sein. Die Wurzeln haben somit entgegengesetzte Zeichen. Die zweite Wurzel ist also negativ, und da sie dem absoluten Werte nach < 1 ist, so können wir sie mit $-\frac{1}{x'}$ bezeichnen, wo x' positiv und > 1 ist. Wir erhalten dann

$$\frac{Q_k}{x'^2} - \frac{Q_{k-1} - P_k}{x'} - P_{k-1} = 0,$$

und daraus folgt

$$x' = \frac{P_k x' + Q_k}{P_{k-1} x' + Q_{k-1}}.$$

x' ist also ebenfalls ein periodischer Kettenbruch, dessen Periode aus k Quotienten besteht, und da diese Periode durch Entwicklung des rationalen Bruchs $\frac{P_k}{P_{k-1}}$ erhalten wird, dessen

vorletzter Näherungsbruch $\frac{Q_k}{Q_{k-1}}$ ist, so ist nach §. 59 die Periode von x' die Umkehrung derjenigen von x .

Beispiel. Der in §. 64 betrachtete Kettenbruch

$$(\overline{1, 2}, 1, \dots)$$

stellt die Wurzel

$$x = \frac{1 + \sqrt{3}}{2}$$

der Gleichung

$$x^2 - x = \frac{1}{2}$$

dar. Wenn wir die andere Wurzel

$$\frac{1 - \sqrt{3}}{2},$$

die negativ und < 1 ist, mit $-\frac{1}{x'}$ bezeichnen und x' , d. i.

$$\frac{2}{-1 + \sqrt{3}}$$

in einen Kettenbruch entwickeln, so erhalten wir

$$x' = (\overline{2, 1}, 2, \dots).$$

Wenn der Kettenbruch, den die Entwicklung der positiven Wurzel $x > 1$ liefert, unrein periodisch ist,

$$x = (\alpha', \alpha'_1, \dots, \alpha'_{m-1}, \overline{\alpha, \alpha_1, \dots, \alpha_{k-1}, \alpha, \dots}),$$

so ist

$$x = \frac{P_m x_m + P_{m-1}}{Q_m x_m + Q_{m-1}},$$

wo

$$x_m = (\overline{\alpha, \alpha_1, \dots, \alpha_{k-1}, \alpha, \dots})$$

ein rein periodischer Kettenbruch, also Wurzel einer Gleichung zweiten Grades ist. Wird die zweite Wurzel dieser Gleichung

mit $-\frac{1}{x'_m}$ bezeichnet, so ist, wie wir eben gesehen haben,

$$x'_m = (\overline{\alpha_{k-1}, \alpha_{k-2}, \dots, \alpha_1, \alpha, \alpha_{k-1}, \dots}),$$

und man erhält die zweite Wurzel x' der ersten Gleichung, wenn man in derselben x_m durch $-\frac{1}{x'_m}$ ersetzt. Es ist also

$$x' = \frac{-\frac{P_m}{x'_m} + P_{m-1}}{-\frac{Q_m}{x'_m} + Q_{m-1}} = \frac{P_{m-1}x'_m - P_m}{Q_{m-1}x'_m - Q_m}.$$

Da

$$P_m Q_{m-1} - P_{m-1} Q_m = (-1)^m$$

ist, so haben die Kettenbrüche für x' und x'_m nach §. 63 einen vollständigen und somit auch einen unvollständigen Quotienten α_λ ($\lambda \leq k-1$) gemeinsam. Nun können wir aber eine Periode bei jedem ihrer Glieder beginnen lassen, also

$$\alpha_{\lambda+1}, \alpha_{\lambda+2}, \dots, \alpha_{k-1}, \alpha, \alpha_1, \dots, \alpha_\lambda$$

als Periode von x und

$$\alpha_\lambda, \alpha_{\lambda-1}, \dots, \alpha_1, \alpha, \alpha_{k-1}, \dots, \alpha_{\lambda+1}$$

als Periode von x'_m und somit auch von x' ansehen, und in diesem Sinne ist die Periode von x' die Umkehrung derjenigen von x .

Beispiel. Die oben gefundene Gleichung

$$11x^2 - 18x + 4 = 0$$

hat die beiden Wurzeln

$$x = \frac{9 + \sqrt{37}}{11} = (1, 2, \overline{1}, 2, \overline{3}, 1, \dots),$$

$$x' = \frac{9 - \sqrt{37}}{11} = (0, 3, 1, \overline{3}, \overline{2}, \overline{1}, 3, \dots).$$

§. 67.

Verwandlung der irrationalen Wurzeln einer rein quadratischen Gleichung in Kettenbrüche.

Es sei

$$Ax^2 = B, \text{ also } x = \frac{\sqrt{AB}}{A}.$$

Wir bestimmen die Wurzel der größten unter AB liegenden Quadratzahl und mittels derselben die größte ganze Zahl α , welche $< x$ ist. Dann setzen wir

$$x = \alpha + \frac{-\alpha A + \sqrt{AB}}{A} = \alpha + \frac{1}{x_1},$$

so ist x_1 eine positive Zahl > 1 . Mit dieser verfahren wir, wie es oben in §. 65 gelehrt worden ist. Auf diese Weise wird x in einen Kettenbruch verwandelt.

Beispiel. Aus $13x^2 = 149$ folgt

$$x = \frac{\sqrt{1937}}{13}.$$

Weiter ist $\sqrt{1937} = 44, \dots$, und wir erhalten der Reihe nach

$$\begin{aligned} x &= 3 + \frac{-39 + \sqrt{1937}}{13} = 3 + \frac{1}{x_1}, \\ x_1 &= \frac{39 + \sqrt{1937}}{32} = 2 + \frac{-25 + \sqrt{1937}}{32} = 2 + \frac{1}{x_2}, \\ x_2 &= \frac{25 + \sqrt{1937}}{41} = 1 + \frac{-16 + \sqrt{1937}}{41} = 1 + \frac{1}{x_3}, \\ x_3 &= \frac{16 + \sqrt{1937}}{41} = 1 + \frac{-25 + \sqrt{1937}}{41} = 1 + \frac{1}{x_4}, \\ x_4 &= \frac{25 + \sqrt{1937}}{32} = 2 + \frac{-39 + \sqrt{1937}}{32} = 2 + \frac{1}{x_5}, \\ x_5 &= \frac{39 + \sqrt{1937}}{13} = 6 + \frac{-39 + \sqrt{1937}}{13} = 6 + \frac{1}{x_1}. \end{aligned}$$

Es ist somit

$$x = (3, \overline{2, 1, 1, 2, 6, 2}, \dots).$$

Wenn $x < 1$ ist, so wird der erste unvollständige Quotient Null sein; in diesem Falle entwickeln wir $\frac{1}{x}$ in einen Kettenbruch. Wir setzen also voraus, daß die GröÙe, um deren Kettenbruchentwicklung es sich handelt, positiv und > 1 sei. Dann hat der Kettenbruch, den wir erhalten, folgende Eigenschaften:

1. Er ist periodisch; denn er ist Wurzel einer quadratischen Gleichung.
2. Er ist unrein periodisch; denn nach §. 66, Lehrsatz II. führt ein rein periodischer Kettenbruch zu der Gleichung

$$Q_k x^2 + (Q_{k-1} - P_k)x - P_{k-1} = 0,$$

und da $x > 1$ vorausgesetzt wird, also auch jeder Näherungsbruch > 1 ist, so ist $P_k > Q_k$ und um so mehr $P_k > Q_{k-1}$, d. h. die vorstehende Gleichung ist gemischt quadratisch.

3. Der Periode geht stets nur ein Glied voraus. Dies zu beweisen, nehmen wir an, es sei

$$x = (\alpha', \alpha'_1, \dots, \alpha'_{m-1}, \overline{\alpha, \alpha_1, \dots, \alpha_{k-1}}, \alpha, \dots),$$

d. h. der Periode $\alpha, \alpha_1, \dots, \alpha_{k-1}$ gingen die m Quotienten $\alpha', \alpha'_1, \dots, \alpha'_{m-1}$ voraus. Dann ist

$$x = \frac{P_{m+k} x_{m+k} + P_{m+k-1}}{Q_{m+k} x_{m+k} + Q_{m+k-1}},$$

also

$$x_{m+k} = \frac{Q_{m+k-1} x - P_{m+k-1}}{P_{m+k} - Q_{m+k} x};$$

ebenso ist

$$x = \frac{P_m x_m + P_{m-1}}{Q_m x_m + Q_{m-1}}, \quad \text{also} \quad x_m = \frac{Q_{m-1} x - P_{m-1}}{P_m - Q_m x},$$

und durch Gleichsetzung der Werte von x_{m+k} und x_m erhalten wir die Gleichung, deren Wurzel x ist, nämlich

$$\frac{Q_{m+k-1} x - P_{m+k-1}}{P_{m+k} - Q_{m+k} x} = \frac{Q_{m-1} x - P_{m-1}}{P_m - Q_m x}.$$

Als Produkt Π der Wurzeln dieser Gleichung ergibt sich leicht

$$\Pi = \frac{P_{m+k} P_{m-1} - P_{m+k-1} P_m}{Q_{m+k} Q_{m-1} - Q_{m+k-1} Q_m}$$

oder, bei Anwendung der Formeln des §. 56,

$$\begin{aligned} \Pi &= \\ &= \frac{(P_{m+k-1} \alpha_{m+k-1} + P_{m+k-2}) P_{m-1} - P_{m+k-1} (P_{m-1} \alpha_{m-1} + P_{m-2})}{(Q_{m+k-1} \alpha_{m+k-1} + Q_{m+k-2}) Q_{m-1} - Q_{m+k-1} (Q_{m-1} \alpha_{m-1} + Q_{m-2})} \\ &= \frac{P_{m+k-1} P_{m-1}}{Q_{m+k-1} Q_{m-1}} \cdot \frac{(\alpha_{m+k-1} - \alpha_{m-1}) + \left(\frac{P_{m+k-2}}{P_{m+k-1}} - \frac{P_{m-2}}{P_{m-1}} \right)}{(\alpha_{m+k-1} - \alpha_{m-1}) + \left(\frac{Q_{m+k-2}}{Q_{m+k-1}} - \frac{Q_{m-2}}{Q_{m-1}} \right)}. \end{aligned}$$

Nun ist $\alpha_{m+k-1} - \alpha_{m-1}$ eine positive oder negative ganze Zahl; denn wäre $\alpha_{m+k-1} = \alpha_{m-1}$, so würde die Periode schon eine Stelle früher, als vorausgesetzt wird, beginnen. Ferner ist sowohl

$$\frac{P_{m+k-2}}{P_{m+k-1}} - \frac{P_{m-2}}{P_{m-1}},$$

als auch

$$\frac{Q_{m+k-2}}{Q_{m+k-1}} - \frac{Q_{m-2}}{Q_{m-1}}$$

als Differenz zweier echten Brüche ein echter Bruch. Das Produkt Π ist daher eine positive Zahl, während das Produkt der Wurzeln einer rein quadratischen Gleichung negativ ist. Der Widerspruch fällt weg, wenn $m = 1$ angenommen wird; denn dann wird

$$\Pi = \frac{P_{k+1} - P_k \alpha}{-Q_k},$$

und dieser Ausdruck kann sowohl positiv wie negativ sein. Der Periode geht also ein unvollständiger Quotient voraus.

4. In dem Kettenbruch

$$(\alpha', \overline{\alpha, \alpha_1, \dots, \alpha_{k-1}, \alpha, \dots}),$$

den die Entwicklung von

$$x = \sqrt{\frac{B}{A}}$$

liefert, ist $\alpha_{k-1} = 2\alpha'$, und die übrigen Quotienten $\alpha, \alpha_1, \dots, \alpha_{k-2}$ der Periode bilden eine symmetrische Reihe.

Da nämlich

$$\sqrt{\frac{B}{A}} = (\alpha', \overline{\alpha, \dots, \alpha_{k-1}, \alpha, \dots})$$

ist, so wird

$$\sqrt{\frac{B}{A}} - \alpha' = (0, \overline{\alpha, \dots, \alpha_{k-1}, \alpha, \dots})$$

ein rein periodischer Kettenbruch sein. Nun sind

$$\sqrt{\frac{B}{A}} + \alpha' \quad \text{und} \quad -\left(\sqrt{\frac{B}{A}} - \alpha'\right)$$

die Wurzeln der quadratischen Gleichung

$$x^2 - 2\alpha'x + \left(\alpha'^2 - \frac{B}{A}\right) = 0;$$

folglich wird auch die Entwicklung von

$$\sqrt{\frac{B}{A}} + \alpha'$$

zu einem rein periodischen Kettenbruch führen, und zwar wird die Periode des letzteren nach §. 66, Lehrsatz III die Umkehrung

der Periode von

$$\sqrt{\frac{B}{A}} - \alpha'$$

sein. Aus

$$\sqrt{\frac{B}{A}} - \alpha' = (0, \overline{\alpha, \alpha_1, \dots, \alpha_{k-1}, \alpha, \dots})$$

folgt erstens (durch Addition von $2\alpha'$)

$$\sqrt{\frac{B}{A}} + \alpha' = (\overline{2\alpha', \alpha, \alpha_1, \dots, \alpha_{k-2}, \alpha_{k-1}, \alpha, \dots});$$

zweitens ist aber auch

$$\sqrt{\frac{B}{A}} + \alpha' = (\overline{\alpha_{k-1}, \alpha_{k-2}, \alpha_{k-3}, \dots, \alpha, \alpha_{k-1}, \dots}),$$

und da beide Entwicklungen identisch sein müssen, so ist

$$\alpha_{k-1} = 2\alpha', \alpha_{k-2} = \alpha, \alpha_{k-3} = \alpha_1, \dots,$$

d. h. das letzte Glied der Periode ist $2\alpha'$, und die übrigen Glieder bilden eine symmetrische Reihe.

5. Dem letzten unvollständigen Quotienten $2\alpha'$ einer jeden Periode entspricht der vollständige Quotient

$$\frac{\alpha' + \sqrt{D}}{1},$$

wo $\sqrt{D}$ der Kürze wegen für $\sqrt{\frac{B}{A}}$ geschrieben ist.

Es sei nämlich

$$x_m = \frac{B_m + \sqrt{D}}{A_m}$$

einer der vollständigen Quotienten in der Entwicklung von $\sqrt{D}$. Wir setzen dann nach dem Früheren

$$\frac{B_m + \sqrt{D}}{A_m} = \alpha_m + \frac{B_m - \alpha_m A_m + \sqrt{D}}{A_m} = \alpha_m + \frac{1}{x_{m+1}}$$

und erhalten

$$x_{m+1} = \frac{\alpha_m A_m - B_m + \sqrt{D}}{\frac{1}{A_m} [D - (\alpha_m A_m - B_m)^2]} = \frac{B_{m+1} + \sqrt{D}}{A_{m+1}},$$

so daß

und

$$B_{m+1} = \alpha_m A_m - B_m$$

also

$$A_{m+1} = \frac{1}{A_m} [D - B_{m+1}^2],$$

$$D = B_{m+1}^2 + A_m A_{m+1}$$

ist. Da nun A_m und A_{m+1} positiv sind, so ist

$$B_{m+1}^2 < D, \quad B_{m+1} < \sqrt{D},$$

d. i.

$$\frac{B_{m+1}}{A_{m+1}} \leq \alpha'.$$

Wenn daher die grösste in dem Bruche

$$\frac{B_k + \sqrt{D}}{A_k}$$

enthaltene ganze Zahl $2\alpha'$ sein soll, so muß

$$B_k = \alpha', \quad A_k = 1,$$

also

$$x_k = \frac{\alpha' + \sqrt{D}}{1}$$

sein.

6. Wenn μ eine beliebige ganze positive Zahl bezeichnet und $\frac{P_{\mu k}}{Q_{\mu k}}$ der Näherungsbruch ist, welcher dem letzten unvollständigen Quotienten, d. i. $2\alpha'$, der μ^{ten} Periode entspricht, so ist

$$P_{\mu k}^2 - D Q_{\mu k}^2 = (-1)^{\mu k}.$$

Es ist nämlich

$$\sqrt{D} = \frac{P_{\mu k} x_{\mu k} + P_{\mu k-1}}{Q_{\mu k} x_{\mu k} + Q_{\mu k-1}},$$

also wegen $x_{\mu k} = \alpha' + \sqrt{D}$

$$\sqrt{D} = \frac{P_{\mu k}(\alpha' + \sqrt{D}) + P_{\mu k-1}}{Q_{\mu k}(\alpha' + \sqrt{D}) + Q_{\mu k-1}}.$$

Durch Fortschaffung des Nenners und durch Gleichsetzung der rationalen und der irrationalen Glieder erhält man hieraus die beiden Gleichungen

$$P_{\mu k} \alpha' - D Q_{\mu k} + P_{\mu k-1} = 0,$$

$$Q_{\mu k} \alpha' - P_{\mu k} + Q_{\mu k-1} = 0,$$

aus denen sich durch Elimination von α'

$$P_{\mu k}^2 - D Q_{\mu k}^2 + P_{\mu k-1} Q_{\mu k} - P_{\mu k} Q_{\mu k-1} = 0$$

oder, da

$$P_{\mu k} Q_{\mu k-1} - P_{\mu k-1} Q_{\mu k} = (-1)^{\mu k}$$

ist,

$$P_{\mu k}^2 - D Q_{\mu k}^2 = (-1)^{\mu k}$$

ergibt.

Beispiel. Wir fanden oben

$$\sqrt{\frac{149}{13}} = (3, 2, 1, 1, 2, 6, 2, \dots).$$

Näherungsbrüche:

3	2	1	1	2	6	2	1	1	2	6	...
$\frac{1}{0}$	$\frac{3}{1}$	$\frac{7}{2}$	$\frac{10}{3}$	$\frac{17}{5}$	$\frac{44}{13}$	$\frac{281}{83}$	$\frac{606}{179}$	$\frac{887}{262}$	$\frac{1493}{441}$	$\frac{3873}{1144}$	...

$$44^2 - \frac{149}{13} \cdot 13^2 = 1936 - 1937 = (-1)^5,$$

$$3873^2 - \frac{149}{13} \cdot 1144^2 = 15000129 - 15000128 = (-1)^{10},$$

.....

§. 68.

Die Fermatsche Aufgabe.

Im Jahre 1657 stellte Pierre Fermat zuerst dem Fre-
nicie, dann allen lebenden Mathematikern, namentlich den
englischen, die Aufgabe, die Gleichung

$$x^2 - Ay^2 = 1,$$

in welcher A eine nichtquadratische ganze positive Zahl ist, in ganzen
Zahlen x, y aufzulösen. (Varia Opera mathematica, S. 190
= Oeuvres, Bd. II, S. 333.) Die in der Hauptsache von Lord
Brouncker gefundene und von Johannes Wallis redigierte
Lösung, die in des letzteren Commercium epistolicum 1658
veröffentlicht, auch von Euler in seiner Algebra, Bd. II,
Kap. VII dargelegt worden ist, hat nicht nur den Nachteil, höchst
umständlich zu sein, sondern sie läßt auch nicht erkennen, daß
die Aufgabe immer möglich ist, d. h. daß es außer den auf der
Hand liegenden Werten

$$x = \pm 1, \quad y = 0$$

immer noch andere Zahlen giebt, welche die Gleichung befriedigen. Erst Lagrange hat diesen Beweis geführt und eine genügende Lösung gegeben (Oeuvres, T. I, S. 671). Thatsächlich gelöst ist die Aufgabe übrigens schon von den Indern¹⁾. Sie wird jetzt meist noch nach dem englischen Mathematiker John Pell benannt, durchaus mit Unrecht, da dieser sich nicht das geringste Verdienst um dieselbe erworben hat.

Lagranges Lösung der für die Zahlentheorie wichtigen Gleichung beruht auf der letzten Formel des §. 67. Es sei nämlich $\sqrt{A}$ in einen Kettenbruch entwickelt:

$$\sqrt{A} = (\alpha', \overline{\alpha_1, \dots, \alpha_{k-2}, 2\alpha'}, \alpha, \dots).$$

so daß also die Periode aus den k Quotienten

$$\alpha, \alpha_1, \dots, \alpha_{k-2}, 2\alpha'$$

besteht, so ist für jede der Zahlen $\mu = 1, 2, 3, \dots$

$$P_{\mu k}^2 - A Q_{\mu k}^2 = (-1)^{\mu k}.$$

Wenn nun k eine gerade Zahl ist, so wird die rechte Seite für jeden Wert von μ gleich $+1$ sein, also ist, wenn die Gliederzahl der Periode gerade ist,

$$x = P_{\mu k}, \quad y = Q_{\mu k}$$

für jeden Wert von μ eine Lösung der Aufgabe.

Wenn die Periode dagegen aus einer ungeraden Anzahl von Gliedern besteht, so ist $(-1)^{\mu k}$ nur für gerade Werte von μ gleich $+1$; in diesem Falle sind daher

$$x = P_{\mu k}, \quad y = Q_{\mu k}$$

nur für gerade Werte von μ Lösungen der Fermatschen Aufgabe.

Beispiele. I. (Fermat, l. c.)

$$x^2 - 3y^2 = 1.$$

$$\sqrt{3} = (1, \overline{1, 2}, 1, \dots).$$

¹⁾ Die „cyklische Methode“ der Inder wird von Brahmagupta und Bhāscara gelehrt und auf viele Beispiele angewandt. Siehe Colebrooke, S. 170 ff.; S. 363 ff. Vergl. auch Hankel, Zur Geschichte der Mathematik im Altertum und Mittelalter, S. 200 ff. Die neueste Beleuchtung der Sache giebt H. Koenen in seiner „Geschichte der Gleichung $t^2 - D u^2 = 1$. Leipzig, 1901“.

1	1	2	1	2	1	2	1	2	...
$\frac{1}{0}$	$\frac{1}{1}$	$\frac{2}{1}$	$\frac{5}{3}$	$\frac{7}{4}$	$\frac{19}{11}$	$\frac{26}{15}$	$\frac{71}{41}$	$\frac{97}{56}$	...

Lösungen:

x	2	7	26	97	...
y	1	4	15	56	...

II. (Bhāscara, Vija-Ganita, S. 248.) Welche beiden ganzen Zahlen haben die Eigenschaft, daß das Quadrat ihrer Summe, vermehrt um den Kubus dieser Summe, gleich der doppelten Summe ihrer Kuben ist?

Bhāscara nimmt

$$I = x + y, \quad II = x - y$$

an; dann soll

$$4x^2 + 8x^3 = 4x^3 + 12xy^2,$$

also

$$4x + 4x^2 = 12y^2,$$

$$(2x + 1)^2 = 12y^2 + 1,$$

oder, wenn $2x + 1 = z$ gesetzt wird,

$$z^2 - 12y^2 = 1$$

sein.

$$\sqrt{12} = (3, \overline{2}, 6, 2, \dots).$$

3	2	6	2	6	2	6	...
$\frac{1}{0}$	$\frac{3}{1}$	$\frac{7}{2}$	$\frac{45}{13}$	$\frac{97}{28}$	$\frac{627}{181}$	$\frac{1351}{390}$	...

Lösungen:

z	7	97	1351	...
y	2	28	390	...
x	3	48	675	...
I	5	76	1065	...
II	1	20	285	...

III. Drei aufeinander folgende Heronische Zahlen $a - 1$, a , $a + 1$ zu bestimmen, mit anderen Worten: Für welche ganzzahligen Werte von a wird die Fläche des Dreiecks mit den Seiten $a - 1$, a , $a + 1$ durch eine ganze Zahl ausgedrückt?

Der Ausdruck für den Flächeninhalt

$$J = \frac{a}{4} \sqrt{3(a^2 - 4)}$$

wird rational, nämlich gleich $\frac{3 a k}{4}$, wenn $a^2 - 4 = 3 k^2$ oder

$$a^2 - 3 k^2 = 4$$

angenommen wird. Nun ist leicht einzusehen, daß keine der Zahlen a , k ungerade sein kann. Wäre nämlich eine der Zahlen a , k gerade, die andere ungerade, so würde $a^2 - 3 k^2$ ungerade sein, könnte also nicht den Wert 4 haben, und wenn a sowohl wie k ungerade wäre, so würde

$$a^2 \equiv 1, 3 k^2 \equiv 3, \text{ also } a^2 - 3 k^2 \equiv 2 \pmod{4}$$

sein, $a^2 - 3 k^2$ wäre also nicht durch 4 teilbar. Es ist somit sowohl a , als auch k eine gerade Zahl. Wir setzen

$$a = 2\alpha, \quad k = 2\kappa,$$

dann erhalten wir die in Beispiel I behandelte Gleichung

$$\alpha^2 - 3 \kappa^2 = 1,$$

und diese liefert die Lösungen

$$3, 4, 5; 13, 14, 15; 51, 52, 53; 193, 194, 195;$$

u. s. w.

IV. Welches ist die kleinste Lösung der Gleichung

$$x^2 - 76 y^2 = 1?$$

$$\sqrt{76} = (8, 1, 2, 1, 1, 5, 4, 5, 1, 1, 2, 1, 16, 1, \dots).$$

8	1	2	1	1	5	4	5	1	1	2	1	16
1	8	9	26	35	61	340	1421	7445	8866	16311	41488	57799
0	1	1	3	4	7	39	163	854	1017	1871	4759	6630

Es ist also

$$x = 57799, \quad y = 6630.$$

V. Man erhält

$$\sqrt{a^2 - 1} = (a - 1, \overline{1, 2a - 2, 1, \dots}),$$

$$\sqrt{a^2 + 1} = (a, \overline{2a, 2a, \dots}),$$

$$\sqrt{a^2 - 2} = (a - 1, \overline{1, a - 2, 1, 2a - 2, 1, \dots}),$$

$$\sqrt{a^2 + 2} = (a, \overline{a, 2a, a, \dots}),$$

$$\sqrt{a^2 - a} = (a - 1, \overline{2, 2a - 2, 2, \dots}).$$

Diese Formeln geben die Kettenbrüche für die Quadratwurzeln aus den in der nachstehenden Tabelle enthaltenen Zahlen:

a	1	2	3	4	5	6	7	8	9	10	...
$a^2 - 1$		3	8	15	24	35	48	63	80	99	...
$a^2 + 1$	2	5	10	17	26	37	50	65	82	101	...
$a^2 - 2$			7	14	23	34	47	62	79	98	...
$a^2 + 2$		6	11	18	27	38	51	66	83	102	...
$a^2 - a$				12	20	30	42	56	72	90	...

Wir vervollständigen diese Tabelle für die unter 100 liegenden Zahlen (nach Euler, Comment. arith. coll. I, p. 322):

$$\sqrt{13} = (3, \overline{1, 1, 1, 1, 6, 1, \dots}),$$

$$\sqrt{19} = (4, \overline{2, 1, 3, 1, 2, 8, 2, \dots}),$$

$$\sqrt{21} = (4, \overline{1, 1, 2, 1, 1, 8, 1, \dots}),$$

$$\sqrt{22} = (4, \overline{1, 2, 4, 2, 1, 8, 1, \dots}),$$

$$\sqrt{28} = (5, \overline{3, 2, 3, 10, 3, \dots}),$$

$$\sqrt{29} = (5, \overline{2, 1, 1, 2, 10, 2, \dots}),$$

$$\sqrt{31} = (5, \overline{1, 1, 3, 5, 3, 1, 1, 10, 1, \dots}),$$

$$\sqrt{32} = (5, \overline{1, 1, 1, 10, 1, \dots}),$$

$$\sqrt{33} = (5, \overline{1, 2, 1, 10, 1, \dots}),$$

$$\sqrt{39} = (6, \overline{4, 12, 4, \dots}),$$

$$\sqrt{40} = (6, \overline{3, 12, 3, \dots}),$$

$$\sqrt{44} = (6, \overline{2, 2, 12, 2, \dots}),$$

$$\sqrt{43} = (6, \overline{1, 1, 3, 1, 5, 1, 3, 1, 1, 12, 1, \dots}),$$

$$\sqrt{44} = (6, \overline{1, 1, 1, 2, 1, 1, 1, 12, 1, \dots}),$$

$$\sqrt{45} = (6, \overline{1, 2, 2, 2, 1, 12, 1, \dots}),$$

$$\begin{aligned}
\sqrt{46} &= (6, \overline{1, 3, 1, 1, 2, 6, 2, 1, 1, 3, 1, 12, 1, \dots}), \\
\sqrt{52} &= (7, \overline{4, 1, 2, 1, 4, 14, 4, \dots}), \\
\sqrt{53} &= (7, \overline{3, 1, 1, 3, 14, 3, \dots}), \\
\sqrt{54} &= (7, \overline{2, 1, 6, 1, 2, 14, 2, \dots}), \\
\sqrt{55} &= (7, \overline{2, 2, 2, 14, 2, \dots}), \\
\sqrt{57} &= (7, \overline{1, 1, 4, 1, 1, 14, 1, \dots}), \\
\sqrt{58} &= (7, \overline{1, 1, 1, 1, 1, 1, 14, 1, \dots}), \\
\sqrt{59} &= (7, \overline{1, 2, 7, 2, 1, 14, 1, \dots}), \\
\sqrt{60} &= (7, \overline{1, 2, 1, 14, 1, \dots}), \\
\sqrt{61} &= (7, \overline{1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14, 1, \dots}), \\
\sqrt{67} &= (8, \overline{5, 2, 1, 1, 7, 1, 1, 2, 5, 16, 5, \dots}), \\
\sqrt{68} &= (8, \overline{4, 16, 4, \dots}), \\
\sqrt{69} &= (8, \overline{3, 3, 1, 4, 1, 3, 3, 16, 3, \dots}), \\
\sqrt{70} &= (8, \overline{2, 1, 2, 1, 2, 16, 2, \dots}), \\
\sqrt{71} &= (8, \overline{2, 2, 1, 7, 1, 2, 2, 16, 2, \dots}), \\
\sqrt{73} &= (8, \overline{1, 1, 5, 5, 1, 1, 16, 1, \dots}), \\
\sqrt{74} &= (8, \overline{1, 1, 1, 1, 16, 1, \dots}), \\
\sqrt{75} &= (8, \overline{1, 1, 1, 16, 1, \dots}), \\
\sqrt{76} &= (8, \overline{1, 2, 1, 1, 5, 4, 5, 1, 1, 2, 1, 16, 1, \dots}), \\
\sqrt{77} &= (8, \overline{1, 3, 2, 3, 1, 16, 1, \dots}), \\
\sqrt{78} &= (8, \overline{1, 4, 1, 16, 1, \dots}), \\
\sqrt{84} &= (9, \overline{6, 18, 6, \dots}), \\
\sqrt{85} &= (9, \overline{4, 1, 1, 4, 18, 4, \dots}), \\
\sqrt{86} &= (9, \overline{3, 1, 1, 1, 8, 1, 1, 1, 3, 18, 3, \dots}), \\
\sqrt{87} &= (9, \overline{3, 18, 3, \dots}), \\
\sqrt{88} &= (9, \overline{2, 1, 1, 1, 2, 18, 2, \dots}), \\
\sqrt{89} &= (9, \overline{2, 3, 3, 2, 18, 2, \dots}), \\
\sqrt{91} &= (9, \overline{1, 1, 5, 1, 5, 1, 1, 18, 1, \dots}), \\
\sqrt{92} &= (9, \overline{1, 1, 2, 4, 2, 1, 1, 18, 1, \dots}), \\
\sqrt{93} &= (9, \overline{1, 1, 1, 4, 6, 4, 1, 1, 1, 18, 1, \dots}), \\
\sqrt{94} &= (9, \overline{1, 2, 3, 1, 1, 5, 1, 8, 1, 5, 1, 1, 3, 2, 1, 18, 1, \dots}), \\
\sqrt{95} &= (9, \overline{1, 2, 1, 18, 1, \dots}), \\
\sqrt{96} &= (9, \overline{1, 3, 1, 18, 1, \dots}), \\
\sqrt{97} &= (9, \overline{1, 5, 1, 1, 1, 1, 1, 1, 5, 1, 18, 1, \dots}).
\end{aligned}$$

Anmerkung I. Wenn die Periode des Kettenbruchs, den die Entwicklung von $\sqrt{A}$ liefert, eine gerade Anzahl von Gliedern enthält, so ist die Gleichung

$$x^2 - Ay^2 = -1$$

unmöglich. Besteht die Periode dagegen aus einer ungeraden Anzahl von Gliedern, so geben die Näherungsbrüche, welche dem letzten unvollständigen Quotienten der ersten, dritten, fünften u. s. w. Periode entsprechen, je eine Lösung der Gleichung. Da die Gleichung auch in der Form

$$y^2 = \frac{x^2 + 1}{A}$$

geschrieben werden kann, A also in die Summe zweier teilerfremden Quadrate aufgehen soll, so muß A nach §. 61, Lehrsatz II selbst die Summe zweier Quadrate sein. Diese Bedingung ist für die Lösbarkeit der Gleichung $x^2 - Ay^2 = -1$ erforderlich, aber nicht hinreichend; so ist z. B. die Gleichung

$$x^2 - 34y^2 = -1$$

unmöglich, obschon $34 = 3^2 + 5^2$ ist. [34 steht oben unter den Zahlen $a^2 - 2$, und die Periode von $\sqrt{a^2 - 2}$ hat nach Beispiel V vier Glieder.] Trotz der Bemühungen von Legendre (Théorie des nombres I, §. 7), Lejeune-Dirichlet (Werke I, S. 221) u. a. ist es noch nicht vollständig gelungen, die Bedingungen für die Lösbarkeit der Gleichung $x^2 - Ay^2 = -1$ anzugeben. Was die Zahlen unter 100 betrifft, so ist die Gleichung

möglich für $A = 2, 5, 10, 13, 17, 26, 29, 37, 41, 50, 53,$
 $58, 61, 65, 73, 74, 82, 85, 89, 97,$

unmöglich für alle übrigen.

Anmerkung II. Es sei $x = p, y = q$ die kleinste Lösung der Gleichung $x^2 - Ay^2 = 1$, also

$$p^2 - Aq^2 = 1.$$

Erhebt man dann $p + q\sqrt{A}$ auf die m^{te} Potenz, wo m irgend eine ganze Zahl ist, und vereinigt sowohl die rationalen als auch die irrationalen Teile, so erhält man

$$(p + q\sqrt{A})^m = P + Q\sqrt{A},$$

und die vorgelegte Gleichung wird für jedes m durch die Werte

$$x = P, \quad y = Q$$

befriedigt.

Aus

$$(p + q \sqrt{A})^m = P + Q \sqrt{A}$$

folgt nämlich

$$(p - q \sqrt{A})^m = P - Q \sqrt{A},$$

und durch Multiplikation beider Gleichungen erhält man

$$P^2 - A Q^2 = (p^2 - A q^2)^m = 1^m = 1.$$

Beispiel.

$$\sqrt{8} = (2, \overline{1, 4}, 1, \dots)$$

hat die Näherungsbrüche

2	1	4	1	4	1	4	1	4	...
$\frac{1}{0}$	$\frac{2}{1}$	$\frac{3}{1}$	$\frac{14}{5}$	$\frac{17}{6}$	$\frac{82}{29}$	$\frac{99}{35}$	$\frac{478}{169}$	$\frac{577}{204}$	...

Die kleinste Lösung der Gleichung $x^2 - 8y^2 = 1$ ist also $x = 3$, $y = 1$, und da

$$(3 + 1 \cdot \sqrt{8})^2 = 17 + 6 \sqrt{8},$$

$$(3 + 1 \cdot \sqrt{8})^3 = 99 + 35 \sqrt{8},$$

$$(3 + 1 \cdot \sqrt{8})^4 = 577 + 204 \sqrt{8},$$

.

ist, so sind die folgenden Lösungen

17 und 6, 99 und 35, 577 und 204, . . . ,

was mit dem Ergebnis der Kettenbruchentwicklung übereinstimmt.



Leonhard Euler

(1707 — 1783).

Nach einem Stich von C. T. Riedel.

Sechstes Kapitel.

Potenzreste für Primzahlmoduln.

§. 69.

Berechnung der Potenzreste.

Es sei p eine ungerade Primzahl und a irgend eine durch p nicht teilbare ganze Zahl. Um die Reste der Potenzen

$$1, a, a^2, a^3, \dots$$

für den Modul p zu erhalten, hat man nicht nötig, die Potenzen selbst sämtlich auszurechnen. Man erhält nämlich den Rest von a^{m+1} , indem man den Rest von a^m mit a multipliziert und den Rest des Produkts nimmt.

Beispiele. I. Für den Modul $p = 17$ ist die Reihe der Potenzen von 2 kongruent den Zahlen

$$1, 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 16, 2^5 \equiv 32 \equiv 15, 2^6 \equiv 30 \equiv 13, \\ 2^7 \equiv 26 \equiv 9, 2^8 \equiv 18 \equiv 1.$$

Die achte Potenz liefert also den Rest 1, die neunte den Rest 2, u. s. w. Die Reihe der Potenzreste von 2 für den Modul 17 umfaßt also nur die acht Zahlen 1, 2, 4, 8, 9, 13, 15, 16, die Zahlen 0, 3, 5, 6, 7, 10, 11, 12, 14 dagegen nicht.

II. Für den Modul 19 ist die Reihe der Potenzreste der Zahl 3 folgende:

$$1, 3, 9, 27 \equiv 8, 8 \cdot 3 = 24 \equiv 5, 15, 15 \cdot 3 = 45 \equiv 7, 7 \cdot 3 = 21 \equiv 2, \\ 2 \cdot 3 = 6, 6 \cdot 3 = 18, 18 \cdot 3 = 54 \equiv 16, 16 \cdot 3 = 48 \equiv 10, 10 \cdot 3 \\ = 30 \equiv 11, 11 \cdot 3 = 33 \equiv 14, 14 \cdot 3 = 42 \equiv 4, 4 \cdot 3 = 12, 12 \cdot 3 \\ = 36 \equiv 17, 17 \cdot 3 = 51 \equiv 13, 13 \cdot 3 = 39 \equiv 1.$$

Es ist also erst die Potenz $3^{18} \equiv 1 \pmod{19}$, und die Reihe der Potenzreste von 3 umfaßt für den Modul 19, abgesehen von der Zahl Null, ein vollständiges Restsystem dieses Moduls.

§. 70.

Der Exponent, zu welchem eine Zahl a für den Modul p gehört.

Da es für den Modul p nur die p Reste $0, 1, 2, \dots, p-1$ giebt, während die Reihe der Potenzen einer Zahl a sich unbegrenzt fortsetzen läßt, so können die Potenzreste von a für den Modul p nicht sämtlich von einander verschieden sein. Zunächst ist klar, daß der Rest 0 überhaupt nicht vorkommen kann; denn da a selbst nicht durch p teilbar ist, so kann auch keine Potenz von a durch p teilbar sein. Es bleiben also nur noch $p-1$ Reste möglich, und somit müssen sich unter den p ersten Gliedern der Reihe

$$(1) \quad 1, a, a^2, \dots, a^{p-1}, a^p, \dots$$

wenigstens zwei verschiedene Glieder befinden, welche denselben Rest liefern. Es sei

$$(2) \quad a^k \equiv a^{k'} \pmod{p};$$

darin ist jede der beiden Zahlen k, k' kleiner als p , und wir setzen, was unbeschadet der Allgemeinheit der Betrachtung geschehen kann, $k > k'$ voraus. Wenn wir dann die Kongruenz (2) durch $a^{k'}$ dividieren, was nach §. 34 zulässig ist, so erhalten wir

$$(3) \quad a^{k-k'} \equiv 1 \pmod{p}.$$

Nun ist $k-k'$ kleiner als p und von Null verschieden. Es befindet sich also unter den p ersten Gliedern der Reihe (1) außer dem ersten Gliede selbst wenigstens noch ein Glied a^n , welches für den Modul p den Rest 1 liefert. Möglicherweise enthält das angegebene Intervall mehrere für den Modul p der Einheit kongruente Potenzen von a . Die kleinste Zahl n , für welche

$$a^n \equiv 1 \pmod{p}$$

ist, nennt man den Exponenten, zu welchem a für den Modul p gehört. So z. B. gehört, wie wir oben gefunden

haben, die Zahl 2 für den Modul 17 zum Exponenten 8 und die Zahl 3 für den Modul 19 zum Exponenten 18.

Aus der nachstehenden Tabelle der Potenzreste der Zahlen 2 bis 18 für den Modul 19 geht hervor, daß

zum Exponenten 2 die Zahl 18 gehört,

" " 3 die Zahlen 7, 11,

" " 6 " " 8, 12,

" " 9 " " 4, 5, 6, 9, 16, 17,

" " 18 " " 2, 3, 10, 13, 14, 15

gehören.

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1									
5	6	11	17	9	7	16	4	1									
6	17	7	4	5	11	9	16	1									
7	11	1															
8	7	18	11	12	1												
9	5	7	6	16	11	4	17	1									
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1															
12	11	18	7	8	1												
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1									
17	4	11	16	6	7	5	9	1									
18	1																

Anmerkung: Man beachte, daß nach dieser Tabelle für jeden Wert von α

$$2^\alpha \equiv 10^{18-\alpha}, 3^\alpha \equiv 13^{18-\alpha}, 4^\alpha \equiv 5^{18-\alpha}, 6^\alpha \equiv 16^{18-\alpha},$$

$$7^\alpha \equiv 11^{18-\alpha}, 8^\alpha \equiv 12^{18-\alpha}, 9^\alpha \equiv 17^{18-\alpha}, 14^\alpha \equiv 15^{18-\alpha},$$

und ebenso

$$4^\alpha \equiv 5^{9-\alpha}, 6^\alpha \equiv 16^{9-\alpha}, 9^\alpha \equiv 17^{9-\alpha}, 8^\alpha \equiv 12^{9-\alpha},$$

$$7^\alpha \equiv 11^{9-\alpha} \pmod{19}$$

ist. Sind nämlich a und b zwei zu demselben Exponenten n gehörende Zahlen, deren Produkt $\equiv 1 \pmod{p}$ ist, so hat man

$a^a \cdot b^a \equiv (ab)^a \equiv 1$ oder, da für jede ganze Zahl k

$$b^{nk} \equiv 1 \pmod{p}$$

ist,

$$a^a \cdot b^a \equiv b^{nk}, \text{ folglich } a^a \equiv b^{nk-a} \pmod{p}.$$

§. 71.

Die Periode einer Zahl für einen Modul.

Wir nehmen an, die Zahl a gehöre für den Modul p zum Exponenten n . Dann ist leicht zu beweisen, daß die Potenzen

$$1, a, a^2, \dots, a^{n-1}$$

für diesen Modul inkongruent sein müssen. Hätte man nämlich

$$a^k \equiv a^{k'} \pmod{p},$$

wo jede der beiden Zahlen k, k' kleiner als n und $k > k'$ sein möge, so könnte man, da a und somit auch jede Potenz von a prim zu p ist, nach §. 34 durch $a^{k'}$ dividieren und erhielte

$$a^{k-k'} \equiv 1 \pmod{p}.$$

Das ist aber unmöglich, da die Zahl a zum Exponenten n gehört und $k - k' < n$ ist. Die Potenzen

$$1, a, a^2, \dots, a^{n-1}$$

sind also in der That für den Modul p inkongruent.

Die folgenden Potenzen geben aber wieder genau dieselben Reste in genau derselben Reihenfolge. Es ist nämlich

$$\begin{aligned} a^n &\equiv 1, & a^{n+1} &\equiv a, & a^{n+2} &\equiv a^2, & \dots, & a^{2n-1} &\equiv a^{n-1}, \\ a^{2n} &\equiv 1, & a^{2n+1} &\equiv a, & a^{2n+2} &\equiv a^2, & \dots, & a^{3n-1} &\equiv a^{n-1}, \\ &\dots & & & & & & & \\ a^{kn} &\equiv 1, & a^{kn+1} &\equiv a, & a^{kn+2} &\equiv a^2, & \dots, & a^{(k+1)n-1} &\equiv a^{n-1}, \\ &\dots & & & & & & & \end{aligned}$$

Zunächst leuchtet ohne weiteres ein, daß jede Potenz von a^n , ebenso wie a^n selbst den Rest 1 liefert. Umgekehrt ist aber auch der Exponent s jeder Potenz a^s , welche $\equiv 1 \pmod{p}$ ist, ein Vielfaches von n . Wenn wir nämlich s durch n dividieren und den Quotienten dieser Division q , den Rest, der $< n$ sein wird, r nennen, so ist $s = qn + r$, folglich $a^s = a^{qn} \cdot a^r$, und da $a^s \equiv 1 \pmod{p}$ sein soll und $a^{qn} = (a^n)^q \equiv 1 \pmod{p}$ ist,

so muß auch $a^r \equiv 1 \pmod{p}$ sein. r ist aber kleiner als der Exponent n , zu welchem a gehört. Folglich kann a^r , nur wenn $r = 0$ ist, den Rest 1 liefern. Dann ist aber $s = qn$, d. h. s ein Vielfaches von n .

Weiter ergibt sich, daß zwei Potenzen a^s und a^t von a denselben Rest liefern, wenn $s \equiv t \pmod{n}$ ist. In diesem Falle ist nämlich $s = t + kn$, folglich $a^s = a^t \cdot a^{kn}$ und, da $a^{kn} \equiv 1$ ist, $a^s \equiv a^t \pmod{p}$. Umgekehrt folgt aus der Annahme $a^s \equiv a^t \pmod{p}$, wenn $s > t$ vorausgesetzt wird, durch Division mit a^t , daß $a^{s-t} \equiv 1 \pmod{p}$, also $s - t$ ein Vielfaches von n oder $s \equiv t \pmod{n}$ sein muß.

Wir sehen somit, daß, wenn eine Zahl a für den Modul p zum Exponenten n gehört, die Reste der Potenzen

$$1, a, a^2, \dots, a^{n-1},$$

welche sämtlich von einander verschieden sind, in unveränderter Reihenfolge wiederkehren. Man nennt sie deshalb die Periode der Zahl a für den Modul p . So ist

$$1, 2, 4, 8, 16, 15, 13, 9$$

die Periode der Zahl 2 für den Modul 17.

Aufgaben. I. Den Rest zu bestimmen, den die Potenz a^m für eine gegebene Primzahl p als Modul liefert.

Lösung. Man bestimme den Exponenten n , zu welchem a für den Modul p gehört, und dividiere m durch n . Werden der Quotient und der Rest dieser Division beziehungsweise q und r genannt, so ist $m = qn + r$ und $a^m \equiv a^r \pmod{p}$. Der Rest von a^m ist also mit demjenigen von a^r identisch.

Beispiel. Welchen Rest giebt 3^{3142} bei der Division durch 7? Die Potenzreste von 3 für den Modul 7 sind

$$3, 9 \equiv 2, 6, 18 \equiv 4, 12 \equiv 5, 15 \equiv 1.$$

Es ist also $3^6 \equiv 1 \pmod{7}$, und da $3142 = 6 \cdot 523 + 4$ ist, so erhalten wir

$$3^{3142} = 3^{623 \cdot 6} \cdot 3^4 \equiv 3^4 \equiv 4 \pmod{7}.$$

II. Beweise den folgenden Satz: Wenn die Zahl a für den Modul p zum Exponenten m gehört, so sind die Potenzen

$$a, a^2, a^3, \dots, a^m$$

die Wurzeln der Kongruenz $x^m \equiv 1 \pmod{p}$; sie sind zugleich

die sämtlichen Zahlen, welche zu den Divisoren von m (die Einheit und die Zahl m nicht ausgeschlossen) als Exponenten gehören.

Beispiel. Für den Modul 37 (s. die Tabelle in §. 82) gehört 4 zum Exponenten 18. Die Potenzreste von 4 sind 4, 16, 27, 34, 25, 26, 30, 9, 36, 33, 21, 10, 3, 12, 11, 7, 28, 1, und es gehören zu den Exponenten 1, 2, 3, 6, 9, 18 (den Divisoren von 18) beziehungsweise die Zahlen:

1; 36; 10, 26; 11, 27; 7, 9, 12, 16, 33, 34; 3, 4, 21, 25, 28, 30.

§. 72.

Eulers zweiter Beweis des Fermatschen Satzes.
(Euler, Commentationes arithmet. collectae I, p. 260.)

Es soll bewiesen werden, daß $a^{p-1} \equiv 1 \pmod{p}$, also $p-1$ ein Vielfaches des Exponenten n ist, zu welchem a für den Modul p gehört. Nach §. 70 ist n entweder $= p-1$ oder $< p-1$. Wenn $n = p-1$ ist, so ist der Satz bewiesen. Es sei also $n < p-1$. Wir streichen nun aus der Reihe

(1) $1, 2, 3, \dots, p-1$

alle diejenigen Zahlen, welche mod. p den Potenzen

(2) $a, a^2, a^3, \dots, a^n$

kongruent sind. Da diese Potenzen nach §. 71 inkongruent sind, so fallen auf diese Weise n Zahlen weg.

Es sei jetzt b eine der $p-1-n$ stehen gebliebenen Zahlen; dann sind die Reste der n Produkte

(3) $ab, a^2b, a^3b, \dots, a^nb$

sowohl unter einander als auch von den Resten der Zahlen (2) verschieden. Wäre nämlich $a^k b \equiv a^l b \pmod{p}$, so müßte auch $a^k \equiv a^l$ sein, während die Zahlen (2) inkongruent sind. Hätte man aber $a^k b \equiv a^l$, so würde, wenn $l > k$ vorausgesetzt wird, durch Division mit a^k sich $b \equiv a^{l-k} \pmod{p}$ ergeben, d. h. b wäre der Voraussetzung zuwider ein Glied von (2), und wenn $l < k$ vorausgesetzt wird, so wäre die Kongruenz $a^k b \equiv a^l$ gleichbedeutend mit $a^k b \equiv a^{l+n-k}$, und aus dieser würde, durch Division mit a^k , $b \equiv a^{l+n-k}$ folgen, es müßte also auch in diesem Falle

b ein Glied von (2) sein. Da somit die Reste der Zahlen (3) sowohl untereinander, als auch von den Zahlen (2) verschieden sind, so fallen durch Weglassung derselben aus (1) n weitere Zahlen weg. Es sind jetzt $2n$ Zahlen aus (1) weggefallen, und wenn jetzt die Reihe (1) erschöpft ist, so ist $p - 1 = 2n$, also der Satz bewiesen.

Im entgegengesetzten Falle sei c eine der noch stehen gebliebenen Zahlen; dann wird wie oben bewiesen, daß die n Produkte

$$(4) \quad ac, a^2c, a^3c, \dots, a^nc$$

sowohl untereinander, als auch von den Zahlen (2) verschieden sind. Es läßt sich aber auch leicht darthun, daß die Zahlen (4) von den Zahlen (3) verschieden sein werden. Hätte man nämlich $a^k b \equiv a^l c$ und wäre $k > l$, so würde sich durch Division mit a^l die Kongruenz $a^{k-l} b \equiv c$ ergeben, nach welcher c ein Glied der Reihe (3) sein müßte. Zu demselben Widerspruch würde im Falle $k < l$ die Kongruenz $a^{k+n} b \equiv a^l c$ führen, da man durch Division mit a^l die Kongruenz $a^{k+n-l} b \equiv c$ erhielte und $k + n - l$ ebenso wie im ersten Falle $k - l < n$ ist. Die Reste von (4) sind also n neue Zahlen, und wenn wir dieselben aus (1) fortlassen, so sind im ganzen $3n$ Zahlen in Wegfall gekommen. Wenn jetzt die Reihe (1) erschöpft ist, so ist

$$p - 1 = 3n,$$

also der Fermatsche Satz bewiesen. Im entgegengesetzten Falle erhält man durch Multiplikation der Zahlen (2) mit einer der noch stehen gebliebenen Zahlen n neue von den bereits weggelassenen und untereinander verschiedene Zahlen. Da die Reihe (1) eine endliche Anzahl von Zahlen enthält, so muß sie endlich einmal erschöpft werden, d. h. sie muß auf die dargelegte Weise in k Reihen zerfallen, von denen jede aus n Zahlen besteht, und zwar wird jede Zahl der Reihe (1) einer und nur einer der k Reihen angehören. Es ist also $p - 1 = kn$, d. h. $p - 1$ ist ein Vielfaches von n .

§. 73.

Verteilung der durch p nicht teilbaren Zahlen unter die verschiedenen Divisoren von $p - 1$ als Exponenten.

Da kongruente Zahlen zu demselben Exponenten gehören, so können wir unsere Betrachtung auf die Zahlen

$$1, 2, 3, \dots, p - 1$$

beschränken.

Es sei a irgend eine dieser Zahlen. Dieselbe gehöre für den Modul p zum Exponenten n , d. h. es sei a^n die niedrigste Potenz von a , welche bei der Division durch p den Rest 1 giebt. Wenn dann auch $a^e \equiv 1 \pmod{p}$ ist, so muß nach §. 71 s durch n teilbar sein. Nun ist nach dem Fermatschen Satze

$$a^{p-1} \equiv 1 \pmod{p};$$

folglich ist der Exponent n , zu welchem a gehört, ein Divisor von $p - 1$.

Es fragt sich jetzt, ob auch zu jedem Divisor von $p - 1$ Zahlen gehören, und wie groß eventuell für jeden Divisor die Anzahl dieser Zahlen ist. Diese Frage beantwortet der folgende

Lehrsatz. Zu jedem Divisor d von $p - 1$ gehören $\varphi(d)$ verschiedene, d. i. mod. p inkongruente Zahlen. Mit $\varphi(d)$ wird wie früher die Anzahl der Zahlen bezeichnet, welche prim zu d und nicht größer als d sind.

Beweis. Wir nehmen an, es gebe wenigstens eine Zahl α , die zum Exponenten d gehört, also eine Wurzel der Kongruenz $\alpha^d \equiv 1 \pmod{p}$ ist. Diese Kongruenz kann nach §. 47, Lehrsatz I nicht mehr als d Wurzeln haben, und da sie durch jeden der mod. p inkongruenten Werte

$$\alpha, \alpha^2, \alpha^3, \dots, \alpha^d$$

befriedigt wird, so sind diese ihre sämtlichen Wurzeln. Es werden sich somit alle zum Exponenten d gehörenden Zahlen unter den Potenzen

$$\alpha, \alpha^2, \alpha^3, \dots, \alpha^d$$

vorfinden.

Wir wollen nun zeigen, daß jede dieser Potenzen, wofern ihr Exponent prim zu d ist, auch wirklich zum Exponenten d gehört, sonst aber nicht.

Es sei α^k eine solche Potenz, also k prim zu d . Nach §. 40 können wir eine Zahl m bestimmen, für welche $km \equiv 1 \pmod{d}$ ist. Wenn nun α^k nicht zum Exponenten d , sondern zu einem Exponenten e gehörte, so müßte, da $\alpha^{kd} \equiv 1 \pmod{p}$ ist, $e < d$ sein. Es wäre dann $\alpha^{ke} \equiv 1$, somit auch $\alpha^{km} \equiv 1$ und, da $\alpha^{km} \equiv \alpha$ ist, $\alpha^e \equiv 1 \pmod{p}$. Die Zahl α würde also zu einem Exponenten e gehören, der kleiner als d wäre, und das wider-

spricht der Voraussetzung. In diesem Falle gehört demnach die Potenz α^k in der That zum Exponenten d .

Wenn dagegen k und d einen grössten gemeinschaftlichen Divisor $\delta > 1$ haben, so ist

$$(\alpha^{\frac{k}{\delta}})^d = (\alpha^k)^{\frac{d}{\delta}} \equiv 1 \pmod{p},$$

und da k und $\frac{d}{\delta}$ prim zu einander sind, so gehört α^k schon zum Exponenten $\frac{d}{\delta}$.

Wenn es also überhaupt eine Zahl α giebt, die zum Exponenten d gehört, so werden zu diesem Exponenten alle diejenigen Glieder der Reihe

$$\alpha, \alpha^2, \alpha^3, \dots, \alpha^d$$

gehören, deren Exponenten prim zu d sind; die Anzahl dieser Glieder ist nach der Definition $\varphi(d)$, und somit haben wir das Resultat gewonnen, daß zum Divisor d von $p - 1$ entweder gar keine oder $\varphi(d)$ Zahlen gehören. Wir wollen nun die Anzahl der zum Exponenten d wirklich gehörenden Zahlen mit $\psi(d)$ bezeichnen. Dann ist also $\psi(d)$ entweder Null oder gleich $\varphi(d)$.

Die verschiedenen Divisoren von $p - 1$ seien jetzt

$$d_1, d_2, \dots, d_n.$$

Da nun die Zahlen

$$1, 2, 3, \dots, p - 1$$

sämtlich sich nur unter diese Divisoren als Exponenten verteilen, so muß

$$\psi(d_1) + \psi(d_2) + \dots + \psi(d_n) = p - 1$$

sein. Nach §. 19, Lehrsatz II ist aber auch

$$\varphi(d_1) + \varphi(d_2) + \dots + \varphi(d_n) = p - 1,$$

somit

$$\psi(d_1) + \psi(d_2) + \dots + \psi(d_n) = \varphi(d_1) + \varphi(d_2) + \dots + \varphi(d_n).$$

Jedes Glied der linken Seite ist aber entweder Null oder gleich dem entsprechenden Gliede der rechten Seite, nie größer als dasselbe, und daher kann die letzte Gleichung nur bestehen, wenn kein Glied ihrer linken Seite $= 0$, sondern allgemein

$$\psi(d) = \varphi(d)$$

ist. Zu jedem Divisor d von $p - 1$ gehören demnach $\varphi(d)$ Zahlen der Reihe

$$1, 2, 3, \dots, p - 1.$$

Beispiel. Es sei $p = 61$. Die Zahl $p - 1 = 60$ hat die 12 Divisoren

$$1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60,$$

und die folgende Tabelle zeigt, wie sich die Zahlen

$$1, 2, 3, \dots, 59, 60$$

unter diese Divisoren als Exponenten verteilen.

Divisor		Zugehörige Zahlen							
1	1								
2	60								
3	13	47							
4	11	50							
5	9	20	34	58					
6	14	48							
10	3	27	41	52					
12	21	29	32	40					
15	12	15	16	22	25	42	56	57	
20	8	23	24	28	33	37	38	53	
30	4	5	19	36	39	45	46	49	
60	2	6	7	10	17	18	26	30	
	31	35	43	44	51	54	55	59.	

Aufgabe. Es sind die Zahlen gegeben, welche beziehungsweise zu den Exponenten m und n gehören. Man soll die zu dem kleinsten Vielfachen v von m und n gehörenden Zahlen ermitteln.

Lösung. Es seien erstens m und n prim zu einander. Wenn dann a eine der Zahlen ist, die zu m gehören, b eine derjenigen, die zu n gehören, so gehört das Produkt ab zum Exponenten $v = mn$.

Aus den Annahmen $a^m \equiv 1$, $b^n \equiv 1$ folgt nämlich $a^{mn} \equiv 1$, $b^{mn} \equiv 1$, also $(ab)^{mn} \equiv 1 \pmod{p}$. Es ist daher nur zu zeigen, daß der Exponent, zu welchem ab gehört, nicht kleiner als mn sein kann. Wird dieser Exponent mit k bezeichnet, so ist $(ab)^k \equiv 1$, also auch $(ab)^{mk}$, d. i. $a^{mk} \cdot b^{mk} \equiv 1$ und, weil

$a^{mk} \equiv 1$ ist, $b^{mk} \equiv 1 \pmod{p}$. Da nun b zum Exponenten n gehört, so muß n in mk aufgehen. m ist aber prim zu n ; folglich muß k durch n teilbar sein.

Ebenso läßt sich zeigen, daß k auch durch m teilbar sein muß. k ist also durch das Produkt mn teilbar und kann daher nicht kleiner als dieses Produkt sein.

Wir werden somit alle zu mn gehörenden Zahlen ab erhalten, indem wir jede Zahl a mit jeder Zahl b multiplizieren.

Beispiel. Für den Modul 61 gehören zum Exponenten 3 die Zahlen 13, 47, zum Exponenten 10 die Zahlen 3, 27, 41, 52, also zum Exponenten $3 \cdot 10 = 30$

$$\begin{aligned} 13 \cdot 3 &\equiv 39, & 13 \cdot 27 &\equiv 46, & 13 \cdot 41 &\equiv 45, & 13 \cdot 52 &\equiv 5, \\ 47 \cdot 3 &\equiv 19, & 47 \cdot 27 &\equiv 49, & 47 \cdot 41 &\equiv 36, & 47 \cdot 52 &\equiv 4. \end{aligned}$$

Wenn m und n zweitens den größten gemeinschaftlichen Divisor $\delta > 1$ haben, etwa $m = \mu\delta$, $n = \nu\delta$ ist, so wird

$$v = \mu\nu\delta$$

sein. Zerlegt man nun v in zwei Faktoren n_1, m_1 , die prim zu einander sind, und von denen der erste in m , der zweite in n aufgeht, so gehört $a^{\frac{m}{m_1}}$ zum Exponenten m_1 , $b^{\frac{n}{n_1}}$ zum Exponenten n_1 , also $a^{\frac{m}{m_1}} \cdot b^{\frac{n}{n_1}}$ zum Exponenten $m_1 n_1 = v$. Die Verbindung aller Werte von $a^{\frac{m}{m_1}}$ mit allen Werten von $b^{\frac{n}{n_1}}$ liefert alle zu v gehörenden Zahlen.

Beispiel. Für den Modul 61 gehören zu $m = 12$ die Zahlen 21, 29, 32, 40, zu $n = 15$ die Zahlen 12, 15, 16, 22, 25, 42, 56, 57. Hier ist

$$m = 3 \cdot 4, \quad n = 3 \cdot 5, \quad v = 3 \cdot 4 \cdot 5 = 60, \quad 60 = 12 \cdot 5,$$

also

$$\frac{m}{m_1} = \frac{12}{12} = 1, \quad \frac{n}{n_1} = \frac{15}{5} = 3,$$

und da mod. 61

$$\begin{aligned} 12^3 &\equiv 15^3 \equiv 20, & 16^3 &\equiv 25^3 \equiv 9, \\ 22^3 &\equiv 42^3 \equiv 34, & 56^3 &\equiv 57^3 \equiv 58 \end{aligned}$$

ist, so erhält man die zum Exponenten 60 gehörenden Zahlen, indem man jede der vier Zahlen 21, 29, 32, 40 mit jeder der vier Zahlen 20, 9, 34, 58 multipliziert und den Rest mod. 61

jedes Produkts nimmt. Man überzeuge sich, daß auf diese Weise die in der vorhergehenden Tabelle angegebenen 16 Zahlen wirklich entstehen.

§. 74.

Produkt der zu demselben Exponenten gehörenden Zahlen.

Zu den Divisoren 1 und 2 von $p - 1$ gehört nur je eine Zahl. Für alle übrigen Divisoren gilt der

Lehrsatz. Das Produkt aller zu einem Divisor d von $p - 1$ gehörenden Zahlen ist $\equiv 1 \pmod{p}$.

Beweis. Es sei α eine zu d gehörende Zahl; dann gehört auch α^m zu d , wofern m prim zu d ist. In diesem Falle ist aber auch $d - m$ prim zu d , also gehört auch α^{d-m} zum Exponenten d . Wäre nun $m = d - m$, so würde $d = 2m$ sein, und da der Fall $d = 2$, $m = 1$ ausgeschlossen ist, so müßte im Widerspruch mit der Voraussetzung d durch m teilbar sein. $d - m$ und m sind somit ungleich, und da

$$\alpha^m \cdot \alpha^{d-m} = \alpha^d \equiv 1 \pmod{p}$$

ist, so lassen sich die zu d gehörenden Zahlen in der Weise in Gruppen von je zweien zusammenstellen, daß das Produkt der beiden Zahlen jeder Gruppe den Rest 1 liefert. Es ist somit auch das Produkt aller zu d gehörenden Zahlen $\equiv 1 \pmod{p}$.

Beispiel. Für den Modul 61 gehören zum Exponenten 10 die Zahlen 3, 27, 41, 52 oder, was dasselbe ist, die Reste der Potenzen 3^1 , 3^3 , 3^9 , 3^7 , und da sowohl $3^1 \cdot 3^9 = 3^{10}$, als auch $3^3 \cdot 3^7 = 3^{10}$ für den Modul 61 nach Voraussetzung den Rest 1 liefert, so ist das Produkt aller vier zum Exponenten 10 gehörenden Zahlen $\equiv 1 \pmod{61}$.

§. 75.

Primitive Wurzeln (Euler, Commentationes arithmet. coll. I, S. 516).

Da $p - 1$ ein Divisor von $p - 1$ ist, so lehrt der in §. 73 bewiesene Satz, daß die Reihe

(1) $1, 2, 3, \dots, p-1$

$\varphi(p-1)$ Zahlen enthält, welche zum Exponenten $p-1$ gehören, d. h. Zahlen, von denen die $(p-1)^{\text{te}}$, aber keine niedrigere Potenz für den Modul p den Rest 1 giebt. Jede dieser $\varphi(p-1)$ Zahlen wird eine primitive Wurzel von p genannt.

Es sei g eine primitive Wurzel von p ; dann sind nach §. 71 die Reste der $p-1$ Potenzen

(2) $1, g, g^2, \dots, g^{p-2}$

sämtlich voneinander und von Null verschieden, stimmen also in irgend einer Reihenfolge mit den Zahlen (1) überein. Wenn es sich demnach um die Kongruenz in Beziehung auf den Modul p handelt, so kann jede der Zahlen (1), also überhaupt jede durch p nicht teilbare ganze Zahl durch eine Potenz einer primitiven Wurzel g ersetzt werden.

Beispiel. Nach der Tabelle des §. 73 ist 2 eine primitive Wurzel von 61, und die Zahlen von 1 bis 60 sind den in der nachstehenden Tabelle angegebenen Potenzen von 2 für den Modul 61 kongruent.

Zahl	Potenz	Zahl	Potenz	Zahl	Potenz	Zahl	Potenz	Zahl	Potenz	Zahl	Potenz
1	2^0	11	2^{13}	21	2^{35}	31	2^{59}	41	2^{54}	51	2^{55}
2	2^1	12	2^8	22	2^{16}	32	2^5	42	2^{56}	52	2^{42}
3	2^4	13	2^{40}	23	2^{57}	33	2^{21}	43	2^{43}	53	2^{33}
4	2^7	14	2^{50}	24	2^9	34	2^{46}	44	2^{17}	54	2^{19}
5	2^{22}	15	2^{28}	25	2^{44}	35	2^{11}	45	2^{34}	55	2^{37}
6	2^7	16	2^4	26	2^{41}	36	2^{14}	46	2^{58}	56	2^{52}
7	2^{10}	17	2^{47}	27	2^{18}	37	2^{39}	47	2^{20}	57	2^{32}
8	2^3	18	2^{13}	28	2^{51}	38	2^{27}	48	2^{10}	58	2^{36}
9	2^{12}	19	2^{26}	29	2^{15}	39	2^{48}	49	2^{38}	59	2^{31}
10	2^{23}	20	2^{74}	30	2^{39}	40	2^{25}	50	2^{45}	60	2^{30}

Aufgabe. Aus einer primitiven Wurzel g der Primzahl p alle übrigen primitiven Wurzeln von p zu berechnen.

Lösung. Wir haben in §. 73 allgemein bewiesen, daß, wenn die Zahl α zum Exponenten d gehört, auch jede Potenz α^k , deren Exponent k prim zu d ist, zu d gehören wird. Es werden also alle Potenzen von g , deren Exponenten prim zu

$p - 1$ sind, primitive Wurzeln von p sein. Da es $\varphi(p - 1)$ solcher Potenzen giebt, und da auch die Anzahl der primitiven Wurzeln von p gleich $\varphi(p - 1)$ ist, so werden die Reste jener Potenzen die sämtlichen primitiven Wurzeln von p sein.

Beispiel. 2 ist primitive Wurzel von 61. Nun sind prim zu 60 die 16 Zahlen

1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59;

folglich hat 61 die 16 primitiven Wurzeln

$$\begin{aligned} 2^1 &\equiv 2, & 2^7 &\equiv 6, & 2^{11} &\equiv 35, & 2^{13} &\equiv 18, & 2^{17} &\equiv 44, & 2^{19} &\equiv 54, \\ 2^{23} &\equiv 10, & 2^{29} &\equiv 30, & 2^{31} &\equiv 59, & 2^{37} &\equiv 55, & 2^{41} &\equiv 26, & 2^{43} &\equiv 43, \\ & & 2^{47} &\equiv 17, & 2^{49} &\equiv 7, & 2^{53} &\equiv 51, & 2^{59} &\equiv 31. \end{aligned}$$

§. 76.

Berechnung einer primitiven Wurzel der Primzahl p .

Um eine primitive Wurzel von p zu ermitteln, wähle man eine durch p nicht teilbare, möglichst kleine Zahl a und bestimme den Exponenten k , zu welchem sie für den Modul p gehört. k ist nach §. 73 ein Divisor von $p - 1$. Ergiebt sich $k = p - 1$, so ist die Aufgabe gelöst, da dann a eine primitive Wurzel von p ist. Wenn dagegen $k < p - 1$ ist, so wähle man eine Zahl b , die sich unter den Potenzresten von a nicht vorfindet, und bestimme den Exponenten k' , zu welchem b gehört.

Nun kann k' kein Divisor von k sein, denn sonst würde aus

$b^{k'} \equiv a^k (\equiv 1)$ sich $b \equiv a^{\frac{k}{k'}} \pmod{p}$ ergeben, b wäre also der Voraussetzung zuwider ein Potenzrest von a . Dagegen kann k' ein Vielfaches von k sein. In diesem Falle gehört b zu einem größeren Exponenten als a , und da wir eine zum größten Exponenten, nämlich zu $p - 1$ gehörende Zahl suchen, so sind wir unserm Ziele näher gekommen. Wir haben dann den Exponenten zu bestimmen, zu welchem eine dritte Zahl gehört, die sich nicht unter den Potenzresten von b und daher auch nicht unter denjenigen von a vorfindet, und weiter in der im Folgenden angegebenen Weise zu verfahren.

Wenn k' kein Vielfaches von k ist, so nehmen wir das kleinste Vielfache v der Zahlen k, k' und bestimmen eine Zahl c , welche zum Exponenten v gehört (Aufgabe des §. 73). Wenn $v = p - 1$

§. 76. Berechnung einer primitiven Wurzel der Primzahl p . 241

ist, so ist c eine primitive Wurzel von p . Im entgegengesetzten Falle haben wir eine Zahl d zu wählen, die sich unter den Potenzresten von c nicht vorfindet, den Exponenten k'' zu suchen, zu welchem d gehört, und — falls auch $k'' < p - 1$ sein sollte — eine Zahl zu bestimmen, welche zu dem kleinsten Vielfachen von v und k'' als Exponenten gehört. Da wir so zu Zahlen gelangen, die zu immer grösseren Exponenten gehören, so werden wir schliesslich eine primitive Wurzel von p erhalten.

Beispiele. I. Es soll eine primitive Wurzel von 41 bestimmt werden. Die Potenzreste von 2 sind

2, 4, 8, 16, 32, 23, 5, 10, 20, 40, 39, 37, 33, 25, 9, 18, 36, 31, 21, 1.

Die Zahl 2 gehört also zum Exponenten 20. Unter den Potenzresten von 2 ist 3 nicht enthalten. Die Potenzreste von 3 sind

3, 9, 27, 40, 38, 32, 14, 1.

Die Zahl 3 gehört somit zum Exponenten 8. Das kleinste Vielfache von 20 und 8 ist $40 = 5 \cdot 8$, und da

$$\frac{20}{5} = 4, \quad \frac{8}{8} = 1$$

ist, so ergibt sich als primitive Wurzel von 41 die Zahl

$$2^4 \cdot 3^1 = 48 \equiv 7 \pmod{41}.$$

II. Für den Modul 73 sind die Potenzreste von 2

2, 4, 8, 16, 32, 64, 55, 37, 1.

Somit gehört 2 zum Exponenten 9. Die Potenzreste von 3 sind

3, 9, 27, 8, 24, 72, 70, 64, 46, 65, 49, 1.

Somit gehört 3 zum Exponenten 12. Das kleinste Vielfache von 9 und 12 ist $36 = 9 \cdot 4$, und da

$$\frac{9}{9} = 1, \quad \frac{12}{4} = 3$$

ist, so gehört $2^1 \cdot 3^3 = 54$ zum Exponenten 36.

Die Potenzreste von 54 sind

54, 69, 3, 16, 61, 9, 48, 37, 27, 71, 38, 8, 67, 41, 24, 55, 50, 72, 19, 4, 70, 57, 12, 64, 25, 36, 46, 2, 35, 65, 6, 32, 49, 18, 23, 1.

[Man beachte, dass sich unter den Potenzresten von 54 die von 2 und die von 3 vorfinden müssen.] Die kleinste unter diesen

Potenzresten nicht vorkommende Zahl ist 5, und die Rechnung ergibt, daß erst die 72. Potenz von 5 den Rest 1 (mod. 73) liefert, daß also 5 eine (und zwar die kleinste) primitive Wurzel von 73 ist.

Anmerkung I. Wenn a zum Exponenten $\frac{p-1}{2}$ gehört und $\frac{p-1}{2}$ eine ungerade Zahl ist, so ist $-a \equiv p-a$ eine primitive Wurzel von p .

Die Reste von $-a$ stimmen nämlich, abgesehen von den Vorzeichen der ungeraden Potenzen, mit denen von $+a$ überein, und da $a^{\frac{p-1}{2}} \equiv +1$ und $\frac{p-1}{2}$ ungerade ist, so wird

$$(-a)^{\frac{p-1}{2}} \equiv -1,$$

also erst

$$(-a)^{p-1} \equiv +1 \pmod{p}$$

sein.

Will man die Potenzreste von $-a$ haben, so schreibt man diejenigen von $+a$ zweimal hin, giebt jeder Potenz mit ungeradem Exponenten das Zeichen $-$ und ersetzt sodann jeden negativen Rest durch die kleinste ihm kongruente positive Zahl.

Beispiel. Für den Modul 43 gehört 9 zum Exponenten 21, also $-9 \equiv 34$ zum Exponenten 42. Die Zahl 34 ist somit eine primitive Wurzel von 43.

Die Potenzreste von $+9$ für den Modul 43 sind

$$\begin{aligned} &9, 38, 41, 25, 10, 4, 36, 23, 35, 14, 40, \\ &16, 15, 6, 11, 13, 31, 21, 17, 24, 1; \end{aligned}$$

folglich sind diejenigen von $-9 \equiv 34$

$$\begin{aligned} &-9, 38, -41, 25, -10, 4, -36, 23, -35, 14, \\ &-40, 16, -15, 6, -11, 13, -31, 21, -17, 24, \\ &-1, 9, -38, 41, -25, 10, -4, 36, -23, 35, \\ &-14, 40, -16, 15, -6, 11, -13, 31, -21, 17, \\ &-24, 1 \end{aligned}$$

oder

$$\begin{aligned} &34, 38, 2, 25, 33, 4, 7, 23, 8, 14, 3, 16, 28, 6, 32, 13, 12, 21, 26, \\ &24, 42, 9, 5, 41, 18, 10, 39, 36, 20, 35, 29, 40, 27, 15, 37, 11, 30, \\ &31, 22, 17, 19, 1. \end{aligned}$$

Anmerkung II. Wenn es sich um die Ermittlung von primitiven Wurzeln recht großer Primzahlen handelt, ist es ratsam, diejenigen Zahlen, von denen man nicht schon im voraus weiß, daß sie unmöglich primitive Wurzeln sein können, der Reihe nach, von der kleinsten anfangend, zu prüfen. Man kann sich dabei darauf beschränken, unter Anwendung einer möglichst weit ausgedehnten Tabelle der Quadratzahlen diejenigen Potenzreste zu berechnen, deren Exponenten die Divisoren von $p - 1$ sind. In vielen Fällen habe ich den folgenden Satz für nützlich gefunden: Wenn $a^m \equiv r$ und $a^{2^m} \equiv r - 1$ ist, so ist

$$a^{2^m} \equiv -1 \pmod{p}.$$

Es ist nämlich

$$a^{2^m} = a^{2^{m-1}} \cdot a^{2^{m-1}} \equiv (r - 1)r \equiv r^2 - r \pmod{p}.$$

Ferner ist ebensowohl $r^2 \equiv a^{2^m}$, als auch $r - 1 \equiv a^{2^{m-1}}$, also $r^2 \equiv r - 1$, folglich $r^2 - r \equiv -1$, d. i.

$$a^{2^m} \equiv -1 \pmod{p}.$$

Aus $2^{971} \equiv 1351$ und $2^{1043} \equiv 1350$ folgt z. B.

$$2^{2013} \equiv -1 \pmod{5827},$$

und da keine niedrigere Potenz von 2 den Rest -1 liefert, so ist erst $2^{6826} \equiv +1$, also 2 eine primitive Wurzel von 5827.

Anmerkung III. Die Aufgabe, aus der Form einer Primzahl p zu schließen, daß eine gegebene Zahl a eine primitive Wurzel derselben sei, ist nur für die Primzahlen $p = 2^n q + 1$, wo n eine ganze Zahl bezeichnet und $q = 1$ oder eine ungerade Primzahl ist, behandelt worden (vergl. Tschebyscheff, Theorie der Kongruenzen, deutsch von Schapira, Berlin 1889, S. 306 bis 313 und G. Wertheim, Primitive Wurzeln der Primzahlen von der Form $2^k q^2 + 1$ u. s. w. Acta mathematica Bd. 20, S. 143 — 152). Der Anhang enthält eine Tabelle der kleinsten primitiven Wurzeln aller Primzahlen unter 6200.

§. 77.

Indizes (Euler, Commentationes arithmet. coll. I, p. 516).

Es sei g eine primitive Wurzel der Primzahl p und a eine beliebige durch p nicht teilbare Zahl. Dann läßt sich, wie wir in §. 75 gesehen haben, ein Exponent α angeben, für welchen

$$a \equiv g^{\alpha} \pmod{p}$$

ist. Man nennt α den Index von a für die Basis g und schreibt $\alpha = {}^g\text{Ind. } a$ oder, wenn die Angabe der Basis nicht erforderlich ist, $\alpha = \text{Ind. } a$. Da nun wegen $g^{p-1} \equiv 1$ auch $g^{k(p-1)} \equiv 1$, also $g^{\alpha} \cdot g^{k(p-1)}$, d. i.

$$g^{\alpha + k(p-1)} \equiv a \pmod{p}$$

ist, so können wir $\alpha + k(p-1)$, d. i. jede Zahl, welche für den Modul $p-1$ kongruent α ist, als Index von a ansehen und

$$\text{Ind. } a \equiv \alpha \pmod{p-1}$$

schreiben.

Beispiel. Für die primitive Wurzel 34 von 43 ist nach §. 76

$$13 \equiv 34^{16} \pmod{43},$$

also

$$\text{Ind. } 13 \equiv 16 \pmod{42}.$$

Lehrsatz. Der Index eines Produkts ist der Summe der Indizes der einzelnen Faktoren nach dem Modul $p-1$ kongruent.

Beweis. Es seien n Zahlen gegeben:

$$a \equiv g^{\alpha}, \quad b \equiv g^{\beta}, \quad \dots, \quad c \equiv g^{\gamma} \pmod{p},$$

dann ist

$$a b \dots c \equiv g^{\alpha + \beta + \dots + \gamma} \pmod{p},$$

also

$$\text{Ind. } (a b \dots c) \equiv \alpha + \beta + \dots + \gamma \pmod{p-1}.$$

Nun sind aber $\alpha, \beta, \dots, \gamma$ beziehungsweise die Indizes von $a, b, \dots, c$, somit ist

$$\text{Ind. } (a b \dots c) \equiv \text{Ind. } a + \text{Ind. } b + \dots + \text{Ind. } c \pmod{p-1}.$$

Zusatz. Der Index der n^{ten} Potenz einer Zahl ist dem n -fachen des Index der Zahl nach dem Modul $p-1$ kongruent.

Beweis. Wird in der letzten Formel jeder der Faktoren $= a$ angenommen, so geht dieselbe, da der Voraussetzung nach n Faktoren vorhanden sind, über in

$$\text{Ind. } a^n \equiv n \text{ Ind. } a \pmod{p-1}.$$

Beispiele. Nach §. 75 ist für $p = 61$ und $g = 2$

$$\text{Ind. } 3 \equiv 6, \quad \text{Ind. } 5 \equiv 22, \quad \text{Ind. } 7 \equiv 49,$$

also Ind. (3.5.7), d. i. Ind. 105 oder $\text{Ind. } 44 \equiv 6 + 22 + 49 \equiv 77 \equiv 17 \pmod{60}$, was nach der Tabelle richtig ist. Ebenso folgt aus $\text{Ind. } 11 \equiv 15$, daß

$\text{Ind. } 11^2 = \text{Ind. } 60 \equiv 30$, $\text{Ind. } 11^3 = \text{Ind. } 660 \equiv \text{Ind. } 50 \equiv 45$ ist, u. s. w.

Wegen der zahlreichen Anwendungen, welche die Indizes finden, ist es wünschenswert, Tafeln zu besitzen, welche für alle unter einer gewissen Grenze liegenden Primzahlen p die Indizes der Zahlen 1, 2, 3, . . . , $p - 1$ und umgekehrt auch die Zahlen liefern, die den Indizes

$$0, 1, 2, \dots, p - 2$$

entsprechen. Die von Jacobi 1839 in Berlin unter dem Titel *Canon arithmeticus* veröffentlichten Tafeln umfassen die Primzahlen unter 1000. Schon vorher hatte nach Hermann Schapira der russische Mathematiker Ostrogradsky Indizestafeln für die unter 200 liegenden Primzahlen seinen Vorlesungen über algebraische und transcendente Analysis beigelegt. Am Ende dieses Werkes sind die Indizestafeln für die in Betracht kommenden Zahlen unter 100 gegeben.

§. 78.

Auflösung der Kongruenz ersten Grades mittels der Indizes.

Es soll die Kongruenz

$$ax \equiv b \pmod{p}$$

aufgelöst werden. Nach dem Lehrsatz des §. 77 ist

$$\text{Ind. } a + \text{Ind. } x \equiv \text{Ind. } b \pmod{p-1},$$

folglich

$$\text{Ind. } x \equiv \text{Ind. } b - \text{Ind. } a \pmod{p-1}.$$

Man findet also x , indem man Ind. a von Ind. b subtrahiert und die Zahl nimmt, welche die erhaltene Differenz zum Index hat.

Auf diese Weise lassen sich alle Kongruenzen ersten Grades mit einer Unbekannten lösen, auch diejenigen, deren Moduln zusammengesetzte Zahlen sind, da man solche Kongruenzen, wie wir in §. 36 gesehen haben, auf Kongruenzen mit Primzahlmoduln zurückführen kann.

Beispiele.

$$\begin{aligned} \text{I. } 39x + 23y &= 2940. \\ 39x &\equiv 2940 \pmod{23}, \\ 16x &\equiv 19 \pmod{23}. \end{aligned}$$

Daraus folgt

$$\text{Ind. } x \equiv \text{Ind. } 19 - \text{Ind. } 16 \pmod{22}$$

oder

$$\begin{aligned} \text{Ind. } x &\equiv 15 - 8 \equiv 7 \pmod{22}, \\ x &\equiv 17 \pmod{23}, \\ x &= 17 + 23k. \end{aligned}$$

$$\begin{aligned} 39 \cdot 17 + 39 \cdot 23k + 23y &= 2940, \\ 39 \cdot 23k + 23y &= 2277, \\ 39k + y &= 99, \\ y &= 99 - 39k. \end{aligned}$$

k	$x = 17 + 23k$	$y = 99 - 39k$
0	17	99
1	40	60
2	63	21.

$$\begin{aligned} \text{II. } 29x &\equiv 301 \pmod{817}, \quad 817 = 19 \cdot 43. \\ 29x &\equiv 301 \pmod{19}, \\ 10x &\equiv 16 \pmod{19}, \\ \text{Ind. } x &\equiv \text{Ind. } 16 - \text{Ind. } 10 \pmod{18}, \\ \text{Ind. } x &\equiv 4 - 17 \equiv -13 \equiv 5 \pmod{18}, \\ x &\equiv 13 \pmod{19}, \\ x &= 13 + 19k. \\ 29(13 + 19k) &\equiv 301 \pmod{19 \cdot 43}, \\ 29 \cdot 19k &\equiv -76 \pmod{19 \cdot 43}, \\ 29k &\equiv -4 \equiv 39 \pmod{43}. \\ \text{Ind. } k &\equiv \text{Ind. } 39 - \text{Ind. } 29 \pmod{42}, \\ \text{Ind. } k &\equiv 33 - 41 \equiv -8 \equiv 34 \pmod{42}, \\ k &\equiv 31 \pmod{43}, \\ k &= 31 + 43l. \end{aligned}$$

$$\begin{aligned} x &= 13 + 19(31 + 43l), \\ x &= 602 + 817l, \\ x &\equiv 602 \pmod{817}. \end{aligned}$$

§. 79.

Die binomische Kongruenz. — Auflösung derselben
mittels der Indizes.

Unter einer binomischen Kongruenz versteht man eine Kongruenz von der Form $ax^n \equiv b \pmod{m}$, wo a, b, m, n ganze Zahlen bedeuten. Wir setzen hier voraus, der Modul sei eine Primzahl p . Dabei können wir p als von 2 verschieden annehmen, da sich nach §. 47, Lehrsatz II der Grad einer Kongruenz unter den Modul hinabdrücken läßt, wir also im Falle $p = 2$ die vorgelegte Kongruenz durch eine Kongruenz ersten Grades ersetzen können. Weiter setzen wir zunächst $a = 1$, $b = 1$ voraus, betrachten also die Kongruenz $x^n \equiv 1 \pmod{p}$, um von derselben einen Satz zu beweisen, der uns später von Nutzen sein wird.

Lehrsatz. Wenn eine Zahl a die Kongruenzen

$$x^m \equiv 1, \quad x^n \equiv 1 \pmod{p}$$

befriedigt und d der größte gemeinschaftliche Divisor von m und n ist, so ist a auch eine Wurzel der Kongruenz

$$x^d \equiv 1 \pmod{p}.$$

Beweis. Es sei

$$m = \mu d, \quad n = \nu d,$$

so daß also μ, ν relative Primzahlen sind. Dann läßt sich eine ganze Zahl k bestimmen, welche der Bedingung

$$\mu k \equiv 1 \pmod{\nu}$$

genügt, und es ist $\frac{\mu k - 1}{\nu}$ eine ganze Zahl, die wir mit y bezeichnen wollen. Somit ist

$$\mu k - \nu y = 1,$$

und daraus folgt durch Multiplikation mit d

$$mk - ny = d.$$

Da nun $a^m \equiv 1 \pmod{p}$ ist, so ist auch $a^{mk} \equiv 1 \pmod{p}$. Ebenso folgt aus $a^n \equiv 1 \pmod{p}$, daß $a^{ny} \equiv 1 \pmod{p}$ sein

wird. Es ist also

$$a^{mk} \equiv a^{nv} \pmod{p}.$$

Nun ist aber a und somit auch jede Potenz von a prim zu p , da sonst $a^m \equiv 0$ (nicht $\equiv 1$) sein würde. Wir können folglich die letzte Kongruenz durch a^{nv} dividieren und erhalten

$$a^{mk-nv} \equiv 1 \pmod{p}$$

oder, was dasselbe ist,

$$a^d \equiv 1 \pmod{p},$$

und das war zu beweisen.

Zusatz. Wenn d der grösste gemeinschaftliche Divisor von m und $p - 1$ ist, so hat die Kongruenz

$$x^m \equiv 1 \pmod{p}$$

d Wurzeln, und diese genügen sämtlich auch der Kongruenz

$$x^d \equiv 1 \pmod{p}.$$

Beweis. Wird im vorhergehenden Satze $n = p - 1$ angenommen, so lehrt derselbe, da jede der $p - 1$ Zahlen

$$1, 2, 3, \dots, p - 1$$

nach dem Fermatschen Satze der Kongruenz $x^{p-1} \equiv 1 \pmod{p}$ genügt, daß eine Zahl, welche eine Wurzel der Kongruenz $x^m \equiv 1 \pmod{p}$ ist, auch Wurzel von $x^d \equiv 1 \pmod{p}$ sein muß, wenn — wie hier vorausgesetzt wird — d der grösste gemeinschaftliche Divisor von m und $p - 1$ ist.

Wenn umgekehrt $a^d \equiv 1 \pmod{p}$ ist, so ist auch $(a^d)^{\frac{m}{d}}$, d. i. $a^m \equiv 1 \pmod{p}$, also a eine Wurzel der Kongruenz

$$x^m \equiv 1 \pmod{p}.$$

Somit haben die Kongruenzen

$$x^m \equiv 1, \quad x^d \equiv 1 \pmod{p}$$

genau dieselben Zahlen zu Wurzeln, und daß die letztere Kongruenz so viele Wurzeln besitzt, als ihr Grad Einheiten enthält, ist in §. 47, Zusatz II bewiesen worden.

Aufgabe. Eine Wurzel der Kongruenz

$$x^d \equiv 1 \pmod{p}$$

zu finden.

Lösung. Bezeichnet ξ eine beliebige, durch die Primzahl p nicht teilbare Zahl, so ist $\xi^{\frac{p-1}{d}}$ eine Wurzel der vorgelegten Kongruenz.

Beispiel. Die Kongruenz $x^4 \equiv 1 \pmod{13}$ hat die Wurzeln
 $2^4 \equiv 8, \quad 3^4 \equiv 27 \equiv 1, \quad 4^4 \equiv 64 \equiv 12, \quad 7^4 \equiv 343 \equiv 5.$

Wir wollen jetzt zeigen, wie die allgemeine binomische Kongruenz mittels der Indizes aufgelöst wird. Es soll die Kongruenz

$$(1) \quad ax^n \equiv b \pmod{p},$$

in welcher a, b ganze Zahlen, n eine positive ganze Zahl und p eine Primzahl bezeichnen, aufgelöst werden. Nimmt man beiderseits die Indizes für eine beliebige Basis, so erhält man

$$(2) \quad n \text{ Ind. } x \equiv \text{Ind. } b - \text{Ind. } a \pmod{p-1},$$

und somit ist die Auflösung von (1) auf die einer Kongruenz ersten Grades mit der Unbekannten $\text{Ind. } x$ zurückgeführt. Wenn die Kongruenz (2) nach §. 34 unmöglich ist, so giebt es auch keinen Wert von x , welcher der Kongruenz (1) genügt. Im entgegengesetzten Falle entspricht jedem sich aus (2) ergebenden Wert von $\text{Ind. } x$ ein aus den Indizestafeln abzulesender Wert von x .

Beispiele. I. Aus $x^9 \equiv 35 \pmod{61}$ folgt

$$9 \text{ Ind. } x \equiv 11 \pmod{60}.$$

Da der größte gemeinschaftliche Divisor 3 von 9 und 60 nicht auch in 11 aufgeht, so ist nach §. 34, Lehrsatz I die letzte Kongruenz unmöglich. Somit ist auch die vorgelegte Kongruenz unlösbar.

II. Aus $19x^{17} \equiv 13 \pmod{61}$ folgt

$$17 \text{ Ind. } x \equiv 40 - 26 \equiv 14 \pmod{60}.$$

Diese Kongruenz liefert für die Unbekannte $\text{Ind. } x$ den Wert

$$\text{Ind. } x \equiv 22 \pmod{60}.$$

Es ist also

$$x \equiv 5 \pmod{61}.$$

III. $67x^6 \equiv 19 \pmod{97}.$

$$6 \text{ Ind. } x \equiv \text{Ind. } 19 - \text{Ind. } 67 \equiv 81 - 57 \equiv 24 \pmod{96},$$

$$\text{Ind. } x \equiv 4 \pmod{16}.$$

Ind. x hat also die 6 für den Modul 96 inkongruenten Werte 4, 20, 36, 52, 68, 84, und diesen entsprechen die sechs verschiedenen Wurzeln der vorgelegten Kongruenz

$$x \equiv 43, 93, 50, 54, 4, 47 \pmod{97}$$

oder

$$x = 97k \pm 4, \pm 43, \pm 47.$$

§. 80.

Die Exponentialkongruenz.

Die Kongruenz

$$a^x \equiv b \pmod{p}$$

liefert

$$x \cdot \text{Ind. } a \equiv \text{Ind. } b \pmod{p-1},$$

sie ist also nur möglich, wenn der grösste gemeinschaftliche Divisor von Ind. a und $p-1$ auch in Ind. b aufgeht. Sie hat in diesem Falle so viele Wurzeln, als dieser grösste gemeinschaftliche Divisor Einheiten enthält.

Beispiele. I.

$$79^x \equiv 8 \pmod{97},$$

$$30^x \equiv 6 \pmod{96},$$

$$5^x \equiv 1 \equiv -15 \pmod{16},$$

$$x \equiv -3 \equiv 13 \pmod{16},$$

$$x = 96k + 13, 29, 45, 61, 77, 93.$$

II. Welche Reste können die Potenzen von 7 für den Modul 19 haben und welche nicht?

Es soll untersucht werden, für welche Werte von y die Kongruenz

$$7^x \equiv y \pmod{19}$$

möglich ist. Dieselbe liefert

$$6x \equiv \text{Ind. } y \pmod{18},$$

sie ist also nur möglich, wenn Ind. y durch 6 teilbar ist. Ind. y kann daher nur die drei Werte 0, 6, 12 haben, und diesen entsprechen die Werte

$$y = 19k + 1, 7, 11.$$

Die Potenzen von 7 können für den Modul 19 also nur die Reste 1, 7, 11 haben. Dieses Resultat läßt sich leicht bestätigen: Es ist mod. 19

$$7^0 \equiv 1, \quad 7^1 \equiv 7, \quad 7^2 = 49 \equiv 11, \quad 7^3 \equiv 77 \equiv 1,$$

also gehört 7 für den Modul 19 zum Exponenten 3, und die Reste 1, 7, 11 kehren in derselben Reihenfolge unaufhörlich wieder.

$$\begin{aligned} \text{III.} \quad & 7^{3x-1} \equiv 53 \pmod{89}, \\ & (3x-1) \text{ Ind. } 7 \equiv \text{Ind. } 53 \pmod{88}, \\ & (3x-1) 81 \equiv 78 \pmod{88}, \\ & (3x-1) 27 \equiv 26 \pmod{88}. \end{aligned}$$

In der Reihe

$$26, \quad 114, \quad 202, \quad 290, \quad 378, \quad \dots$$

ist 378 das erste durch 27 teilbare Glied, und zwar ist

$$378 : 27 = 14,$$

also

$$\begin{aligned} 3x - 1 &\equiv 14 \\ x &\equiv 5 \pmod{88}. \end{aligned}$$

§. 81.

Zusammenhang zwischen den für zwei verschiedene primitive Wurzeln genommenen Indizes einer Zahl.

Nach §. 75 ist

$$25 \equiv 2^{44} \pmod{61},$$

also

$$^2\text{Ind. } 25 \equiv 44 \pmod{60}.$$

Wir stellen uns die Aufgabe, den Index von 25 für die primitive Wurzel 6 zu finden, also die Kongruenz $6^x \equiv 25 \pmod{61}$ zu lösen. Aus

$$6^x \equiv 2^{44} \pmod{61}$$

folgt, wenn beiderseits die Indizes für die (neue) Basis 6 genommen werden,

$$x \equiv 44 \cdot ^6\text{Ind. } 2 \pmod{60}.$$

Es handelt sich also darum, $^6\text{Ind. } 2$ zu bestimmen, d. i. die Kongruenz

$$6^v \equiv 2 \pmod{61}$$

zu lösen. Man erhält, da ${}^2\text{Ind. } 6 = 7$ ist,

$$7y \equiv 1 \pmod{60},$$

und daraus folgt

$$y \equiv 43 \pmod{60}.$$

[In der Reihe 1, 61, 121, 181, 241, 301, ... ist nämlich 301 das erste durch 7 teilbare Glied und $301 : 7 = 43$.] Es ist also

$$x \equiv 44 \cdot 43 \equiv 1892 \equiv 32 \pmod{60},$$

d. h.

$${}^6\text{Ind. } 25 \equiv 32 \pmod{60}.$$

[Probe: $6^2 = 36$, $6^4 = 1296 \equiv 15$, $6^8 \equiv 225 \equiv 42$, $6^{16} \equiv 1764 \equiv -5$, $6^{32} \equiv +25 \pmod{61}$.]

Wir können jetzt, wenn wir wollen, sämtliche für die Basis 2 genommenen Indizes für die Basis 6 nehmen, indem wir jeden der ersteren mit 43 multiplizieren und den Rest des Produkts für den Modul 60 bestimmen. Nach §. 75 ist z. B. mod. 60

für $g = 2$:	folglich für $g = 6$:
Ind. 11 $\equiv 15$,	Ind. 11 $\equiv 15 \cdot 43 \equiv 645 \equiv 45$,
Ind. 12 $\equiv 8$,	Ind. 12 $\equiv 8 \cdot 43 \equiv 344 \equiv 44$,
Ind. 13 $\equiv 40$,	Ind. 13 $\equiv 40 \cdot 43 \equiv 1720 \equiv 40$.

Allgemein nehmen wir an, es seien die Indizes der Zahlen

$$1, 2, 3, \dots, p-1$$

für irgend eine primitive Wurzel g als Basis bestimmt, und es werde verlangt, die Indizes derselben Zahlen für eine zweite primitive Wurzel h zu finden.

Ist

$$a \equiv g^{\alpha}, \quad \text{also} \quad \alpha \equiv {}^g\text{Ind. } a,$$

$$a \equiv h^{\alpha'}, \quad \text{also} \quad \alpha' \equiv {}^h\text{Ind. } a,$$

folglich

$$g^{\alpha} \equiv h^{\alpha'},$$

so ergibt sich, wenn man beiderseits die Indizes für die (neue) Basis h nimmt,

$$\alpha \cdot {}^h\text{Ind. } g \equiv \alpha',$$

d. h.

$${}^h\text{Ind. } a \equiv {}^g\text{Ind. } a \cdot {}^h\text{Ind. } g.$$

Man findet also den Index von a für die neue Basis h , indem man den Index von a für die frühere Basis g mit dem für die neue Basis genommenen Index dieser früheren Basis multipliziert.

Man bestätige diese Regel an den beiden folgenden Tabellen:

I. mod. 11.

Für die primitive Wurzel	ist der Index der Zahl									
	1	2	3	4	5	6	7	8	9	10
2	10	1	8	2	4	9	7	3	6	5
6	10	9	2	8	6	1	3	7	4	5
7	10	3	4	6	2	7	1	9	8	5
8	10	7	6	4	8	3	9	1	2	5

II. mod. 13.

Für die primitive Wurzel	ist der Index der Zahl											
	1	2	3	4	5	6	7	8	9	10	11	12
2	12	1	4	2	9	5	11	3	8	10	7	6
6	12	5	8	10	9	1	7	3	4	2	11	6
7	12	11	8	10	3	7	1	9	4	2	5	6
11	12	7	4	2	3	11	5	9	8	10	1	6

§. 82.

Die Indizes einer Zahl und der Exponent, zu welchem die Zahl gehört.

Es soll der Exponent bestimmt werden, zu welchem eine gegebene Zahl a für die Primzahl p gehört, d. i. der kleinste Wert (außer Null) von x , für welchen

$$a^x \equiv 1 \pmod{p}$$

ist. Nehmen wir beiderseits die Indizes für eine beliebige primitive Wurzel von p , so erhalten wir

$$x \cdot \text{Ind. } a \equiv 0 \pmod{p-1},$$

und daraus folgt, wenn d der größte gemeinschaftliche Divisor von $\text{Ind. } a$ und $p-1$ ist,

$$x \equiv 0 \pmod{p \cdot \frac{p-1}{d}}.$$

Der kleinste Wert von x (außer Null) ist also $\frac{p-1}{d}$, d. h. man findet den Exponenten, zu welchem die Zahl a für den Modul p gehört, indem man $p-1$ durch den grössten gemeinschaftlichen Divisor d von $p-1$ und dem für eine beliebige primitive Wurzel von p genommenen Index von a dividiert.

Beispiel. Für $p = 29$ und die primitive Wurzel 2 ist Ind. 5 = 22. Der grösste gemeinschaftliche Divisor von 28 und 22 ist 2; also gehört 5 für die Primzahl 29 zum Exponenten

$$\frac{28}{2} = 14.$$

Wenn umgekehrt eine Zahl a zum Exponenten $\frac{p-1}{d}$ gehört, so ist d der grösste gemeinschaftliche Divisor von $p-1$ und dem Index von a , gleichgiltig, für welche primitive Wurzel von p der Index genommen sei. Da nämlich für jede primitive Wurzel g

$$g^{\text{Ind. } a} \equiv a \pmod{p}$$

ist und a zum Exponenten $\frac{p-1}{d}$ gehört, so muß

$$g^{\frac{p-1}{d} \text{ Ind. } a} \equiv 1 \pmod{p},$$

also

$$\frac{p-1}{d} \text{ Ind. } a$$

ein Vielfaches von $p-1$ oder Ind. a ein Vielfaches von d sein.

Ferner ist $p-1$ ebenfalls ein Vielfaches von d , da $\frac{p-1}{d}$ als Exponent, zu welchem a gehört, eine ganze Zahl ist. d ist also ein gemeinschaftlicher Divisor von $p-1$ und Ind. a . Es sei

$$\text{Ind. } a = \alpha d, \quad p-1 = \beta d.$$

Wenn wir jetzt zeigen können, daß α und β prim zu einander sind, so ist bewiesen, daß d der grösste gemeinschaftliche Divisor von Ind. a und $p-1$ ist.

Hätten α und β einen grössten gemeinschaftlichen Divisor $\delta > 1$, wäre etwa

$$\alpha = \delta \alpha_1, \quad \beta = \delta \beta_1,$$

wo also α_1, β_1 als prim zu einander vorausgesetzt werden, so wäre

folglich $\text{Ind. } a \equiv \alpha d \equiv \alpha_1 \delta d \pmod{p-1},$

$$a \equiv g^{\alpha_1 \delta d} \pmod{p},$$

und daraus würde durch Erhebung auf die β_1^{te} Potenz

$$a^{\beta_1} \equiv g^{\alpha_1 \beta_1 \delta d} \equiv g^{\alpha_1 \beta d} \equiv g^{\alpha_1 (p-1)} \equiv 1 \pmod{p}$$

folgen, d. h. a würde, der Voraussetzung zuwider, zu einem Exponenten $\beta_1 < \beta$ gehören. Somit ist d in der That der grösste gemeinschaftliche Divisor von $\text{Ind. } a$ und $p-1$.

Aufgabe. Es sind die Indizes der Zahlen

$$1, 2, 3, \dots, p-1$$

für eine beliebige primitive Wurzel von p gegeben. Man soll mittels derselben diese Zahlen unter die Divisoren von $p-1$ als Exponenten verteilen.

Lösung. Man wählt alle Indizes, die mit $p-1$ den grössten gemeinschaftlichen Divisor $\frac{p-1}{d}$ haben. Die zugehörigen Zahlen gehören zum Exponenten d .

Beispiel. Für

$$p = 37, \quad g = 2$$

ergibt sich die Tabelle:

d	$\frac{p-1}{d}$	Indizes, die mit $p-1$ den grössten gemeinschaftlichen Divisor $\frac{p-1}{d}$ haben.								Entsprechende, also zum Exponenten d gehörende Zahlen.					
1	36	36							1						
2	18	18							36						
3	12	12	24						26	10					
4	9	9	27						31	6					
6	6	6	30						27	11					
9	4	4	8	16	20	28	32	16	34	9	33	12	7		
12	3	3	15	21	33			8	23	29	14				
18	2	2	10	14	22	26	34	4	25	30	21	3	28		
36	1	1	5	7	11	13	17	2	32	17	13	15	18		
		19	23	25	29	31	35	35	5	20	24	22	19.		

§. 83.

Summe und Produkt der Glieder der Periode einer Zahl. — Eulers Beweis des Wilsonschen Satzes.

Lehrsatz I. Die Summe aller Glieder der Periode einer Zahl ist $\equiv 0 \pmod{p}$.

Beweis. Wir nehmen an, die Zahl a gehöre für den Modul p zum Exponenten n , habe also die Periode $a, a^2, a^3, \dots, a^n$. Die Summe der Glieder dieser Periode ist bekanntlich

$$\frac{a^{n+1} - a}{a - 1} = \frac{a(a^n - 1)}{a - 1},$$

und da $a^n - 1 \equiv 0 \pmod{p}$ ist, so wird auch diese Summe $\equiv 0 \pmod{p}$ sein, wofern nicht $a - 1 \equiv 0$, d. i. $a \equiv 1 \pmod{p}$ ist, die Periode also aus dem einen Gliede 1 besteht.

Beispiele. I. Für den Modul 13 hat 2 die Periode

$$2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1.$$

Die Summe dieser Zahlen ist $78 \equiv 0 \pmod{13}$.

II. Für denselben Modul hat 3 die Periode 1, 3, 9; die Summe dieser Zahlen ist $13 \equiv 0 \pmod{13}$.

Lehrsatz II. Das Produkt aller Glieder der Periode einer Zahl ist $\equiv +1$ oder $\equiv -1 \pmod{p}$, je nachdem der Exponent n , zu welchem die Zahl gehört, ungerade oder gerade ist.

I. Beweis. Das Produkt der Glieder der Periode

$$a, a^2, a^3, \dots, a^n$$

ist

$$\Pi = a^{\frac{1}{2}n(n+1)}.$$

Wenn nun erstens n ungerade, etwa $n = 2\nu + 1$ ist, so ist

$$n + 1 = 2\nu + 2, \quad \frac{1}{2}(n + 1) = \nu + 1,$$

also $\Pi = a^{n(\nu+1)}$ und, wegen $a^n \equiv 1 \pmod{p}$,

$$\Pi \equiv +1 \pmod{p}.$$

Ist dagegen zweitens n gerade, $n = 2\nu$, so ergibt sich

$$\Pi = a^{\nu(n+1)} = a^{n\nu} \cdot a^\nu$$

und wegen $a^n \equiv 1 \pmod{p}$,

$$\Pi \equiv a^n \equiv a^{\frac{1}{2}n} \equiv -1 \pmod{p}.$$

II. Beweis. Die Glieder der Periode einer zum Exponenten n gehörenden Zahl a werden, abgesehen von der Reihenfolge, erhalten, indem man alle Zahlen nimmt, welche zu den Divisoren von n als Exponenten gehören, wobei die Einheit und die Zahl n selbst nicht auszuschließen sind. Nun ist nach §. 74 das Produkt aller zu einem Divisor von n gehörenden Zahlen, wenn die Divisoren 1 und 2 unberücksichtigt gelassen werden,

$$\equiv +1 \pmod{p}.$$

Zum Exponenten 1 gehört immer die Zahl 1, zum Exponenten 2 die Zahl $p - 1$. Folglich ist das Produkt aller Glieder der Periode einer Zahl $\equiv +1$, wenn der Exponent n den Divisor 2 nicht besitzt, d. h. ungerade ist. Wenn aber n eine gerade Zahl ist, so besitzt sie den Divisor 2; somit ist in diesem Falle das Produkt aller Glieder der Periode der Zahl

$$\equiv p - 1 \equiv -1 \pmod{p}.$$

Beispiele. I. Oben ist die Periode von 2 für den Modul 13 gegeben. Da nun $\pmod{13}$

$$\begin{aligned} 1.12 &\equiv -1, & 2.7 &\equiv +1, & 3.9 &\equiv +1, \\ 4.10 &\equiv +1, & 5.8 &\equiv +1, & 6.11 &\equiv +1 \end{aligned}$$

ist, so ist das Produkt aller Glieder $\equiv -1$.

II. Die Periode von 7 für den Modul 37 ist

$$7, 12, 10, 33, 9, 26, 34, 16, 1.$$

Da nun $\pmod{37}$

$$7.16 \equiv 1, \quad 12.34 \equiv 1, \quad 10.26 \equiv 1, \quad 33.9 \equiv 1$$

ist, so ist das Produkt aller dieser Zahlen $\equiv 1 \pmod{37}$.

Eulers Beweis des Wilsonschen Satzes (Opuscula analytica I, p. 329). — Bezeichnet g eine primitive Wurzel von p , so enthält die Periode von g alle Zahlen

$$1, 2, 3, \dots, p - 1.$$

Da nun in diesem Falle der Exponent, zu welchem g gehört, eine gerade Zahl, nämlich $p - 1$ ist, so ist nach Lehrsatz II

$$1.2.3...(p-1) \equiv -1 \pmod{p},$$

d. h.

$$1.2.3...(p-1) + 1$$

ist durch p teilbar.

§. 84.

Produkt der primitiven Wurzeln einer Primzahl. —
Summe der Indizes einer Zahl.

Die Primzahl 3 hat nur die eine primitive Wurzel 2. Für jede andere Primzahl ist $\varphi(p-1)$, d. i. die Anzahl der primitiven Wurzeln, eine gerade Zahl, und nach dem in §. 74 bewiesenen allgemeinen Satze ist das Produkt aller primitiven Wurzeln $\equiv +1 \pmod{p}$, da sich dieselben in Gruppen von je zweien in der Weise zusammenstellen lassen, daß das Produkt der Wurzeln jeder Gruppe $\equiv +1 \pmod{p}$ ist.

Wir denken uns nun für jede der primitiven Wurzeln den kleinsten positiven, d. i. den zwischen 0 und $p-1$ liegenden Index einer (durch p nicht teilbaren) Zahl a genommen. Für diese Indizes gilt der

Lehrsatz (Paul Epstein, mündliche Mitteilung): Die Summe aller Indizes einer Zahl ist $\frac{1}{2}(p-1)\varphi(p-1)$.

Beweis. Es seien g, g_1 zwei primitive Wurzeln von p , für welche man

$$g \cdot g_1 \equiv 1 \text{ oder } g \cdot g_1 \equiv g^{p-1}, \text{ also } g_1 \equiv g^{p-2} \pmod{p}$$

hat. Ferner sei

$${}^g \text{Ind. } a \equiv \alpha, \quad {}^{g_1} \text{Ind. } a \equiv \alpha_1 \pmod{p-1},$$

also

$$a \equiv g^\alpha \equiv g_1^{\alpha_1} \equiv g^{(p-2)\alpha_1} \pmod{p}.$$

Dann muß

$$\alpha \equiv (p-2)\alpha_1 \equiv (p-1)\alpha_1 - \alpha_1 \equiv -\alpha_1 \pmod{p-1},$$

folglich

$$\alpha + \alpha_1 \equiv 0 \pmod{p-1}$$

sein. Nun soll jeder der Indizes α, α_1 zwischen 0 und $p-1$ liegen. Somit ist

$$\alpha + \alpha_1 = p-1.$$

Wenn also das Produkt zweier primitiven Wurzeln $\equiv 1 \pmod{p}$ ist, so ist die Summe der für dieselben genommenen kleinsten

positiven Indizes einer Zahl gleich $p - 1$. Nun sind $\varphi(p - 1)$ primitive Wurzeln, also $\frac{1}{2}\varphi(p - 1)$ Gruppen von je zweien vorhanden, und da jede Gruppe als Summe der zugehörigen Indizes $p - 1$ liefert, so ist die Summe aller kleinsten positiven Indizes einer Zahl a gleich $\frac{1}{2}\varphi(p - 1) \cdot (p - 1)$.

Beispiel. In der folgenden Tabelle, in der $p = 43$ angenommen ist, sind je zwei primitive Wurzeln, deren Produkt $\equiv 1 \pmod{p}$ ist, z. B. 3 und 29, 5 und 26, u. s. w. nebeneinander gestellt.

Zahl	Index für die primitive Wurzel												
	3	29	5	26	12	18	19	34	20	28	30	33	Summe
4	12	30	24	18	30	12	36	6	6	36	24	18	252
7	35	7	35	7	35	7	35	7	35	7	7	35	252
2	27	15	33	9	15	27	39	3	3	39	33	9	252.

Es ist

$$\varphi(42) = \varphi(6)\varphi(7) = 2 \cdot 6 = 12,$$

$$\frac{1}{2} \cdot 42 = 21 \quad \text{und} \quad 21 \cdot 12 = 252.$$

§. 85.

Summe der zu einem Exponenten gehörenden Zahlen. —
Summe der primitiven Wurzeln einer Primzahl.

Zu dem Divisor 1 von $p - 1$ gehört nur die Zahl 1. Für jeden andern Divisor d von $p - 1$ gilt der

Lehrsatz. Die Summe aller zum Exponenten d gehörenden Zahlen ist $\equiv 0 \pmod{p}$, wenn d durch irgend eine Quadratzahl teilbar ist; sie ist

$$\equiv \pm 1 \pmod{p},$$

wenn d jeden seiner Primfaktoren nur in der ersten Potenz enthält, und zwar ist das obere oder untere Zeichen zu nehmen, jenachdem die Anzahl dieser ungleichen Primfaktoren gerade oder ungerade ist.

Beweis. Es sei

$$d = a^\alpha b^\beta c^\gamma \dots,$$

wo $a, b, c, \dots$ ungleiche Primzahlen, $\alpha, \beta, \gamma, \dots$ ganze positive Zahlen bezeichnen. Da d ein Divisor von $p - 1$ ist, so dürfen wir dann

$$p - 1 = k a^\alpha b^\beta c^\gamma \dots$$

annehmen, wo $k \geq 1$ ist.

Ferner seien

$$A_1, A_2, A_3, \dots$$

die $\varphi(a^\alpha)$ Zahlen, welche zum Exponenten a^α gehören,

$$B_1, B_2, B_3, \dots$$

die $\varphi(b^\beta)$ Zahlen, welche zum Exponenten b^β gehören, u. s. w. Da nun $a^\alpha, b^\beta, \dots$ prim zu einander sind, so gehört jedes Produkt $A B \dots$ nach §. 73 zum Exponenten $a^\alpha b^\beta \dots = d$. Durch Verbindung jeder der Zahlen A mit jeder der Zahlen B u. s. w. entstehen nun $\varphi(a^\alpha) \varphi(b^\beta) \dots = \varphi(d)$ Produkte, und ebenso viele Zahlen gehören nach §. 73 zum Exponenten d . Jene Produkte werden also, wofern sie für den Modul p inkongruent sind, alle zu d gehörenden Zahlen und zwar jede nur einmal darstellen.

Diese Inkongruenz zu beweisen, nehmen wir einmal an, es wäre

$$A_m B_n C_o \dots \equiv A_{m'} B_{n'} C_{o'} \dots \pmod{p}.$$

Durch Erhebung auf die Potenz $b^\beta c^\gamma \dots$ würde sich dann, da

$$B_n^{b^\beta} \equiv C_o^{c^\gamma} \equiv \dots \equiv B_{n'}^{b^\beta} \equiv C_{o'}^{c^\gamma} \equiv \dots \equiv 1 \pmod{p}$$

ist,

$$A_m^{b^\beta c^\gamma \dots} \equiv A_{m'}^{b^\beta c^\gamma \dots} \pmod{p}$$

ergeben. Wir hätten also für eine beliebige primitive Wurzel

$$b^\beta c^\gamma \dots \text{ Ind. } A_m \equiv b^\beta c^\gamma \dots \text{ Ind. } A_{m'} \pmod{p-1},$$

oder, da $p - 1 = k a^\alpha b^\beta c^\gamma \dots$ ist,

$$\text{Ind. } A_m \equiv \text{Ind. } A_{m'} \pmod{k a^\alpha}.$$

Nach §. 82 hat nun sowohl Ind. A_m , als auch Ind. $A_{m'}$, da beide Zahlen $A_m, A_{m'}$ zum Exponenten a^α gehören, mit

$$p - 1 = k a^\alpha b^\beta \dots$$

den größten gemeinschaftlichen Divisor

$$\frac{p-1}{a^\alpha} = k b^\beta c^\gamma \dots$$

Wir können also

$$\text{Ind. } A_m = l k b^\beta c^\gamma \dots, \quad \text{Ind. } A_{m'} = l' k b^\beta c^\gamma \dots$$

setzen, wo jede der Zahlen l, l' prim zu a^α sein muß. Die letzte Kongruenz würde dann

$$l k b^\beta c^\gamma \dots \equiv l' k b^\beta c^\gamma \dots \pmod{k a^\alpha}$$

oder

$$l \equiv l' \pmod{a^\alpha}$$

geben. Es müßte also

$$l' = l + \lambda a^\alpha$$

und

$$\text{Ind. } A_{m'} \equiv l k b^\beta c^\gamma \dots + \lambda k a^\alpha b^\beta c^\gamma \dots$$

$$\equiv \text{Ind. } A_m + \lambda(p-1) \equiv \text{Ind. } A_m \pmod{\overline{p-1}},$$

folglich

$$A_{m'} \equiv A_m \pmod{p}$$

sein, was der Voraussetzung, nach welcher A_m und $A_{m'}$ inkongruent sein sollen, widerspricht. Die Summe aller zum Exponenten $d = a^\alpha b^\beta \dots$ gehörenden Zahlen ist somit identisch mit der Summe aller Produkte $ABC \dots$ oder, was dasselbe ist, mit dem Produkte

$$(A_1 + A_2 + \dots)(B_1 + B_2 + \dots)(C_1 + C_2 + \dots) \dots$$

Um den Rest dieses Produktes für den Modul p zu finden, berechnen wir irgend einen seiner Faktoren, etwa $A_1 + A_2 + \dots$, d. i. die Summe aller zum Exponenten a^α gehörenden Zahlen.

Wenn $\alpha = 1$, also $a^\alpha = a$ ist, so gehören zum Exponenten a^α die Zahlen

$$A, A^2, A^3, \dots, A^{a-1}$$

und da nach §. 83, Lehrsatz I

$$1 + A + A^2 + \dots + A^{a-1} \equiv 0 \pmod{p}$$

ist, so erhalten wir in diesem Falle

$$A + A^2 + \dots + A^{a-1} \equiv -1 \pmod{p}.$$

Wenn weiter $\alpha > 1$ ist, so gehören zu a^α aufser A selbst auch diejenigen Potenzen von A , deren Exponenten prim zu a^α sind, also die Zahlen

$$A, A^2, A^3, \dots, A^{a^\alpha-1}$$

mit Ausschluss von

$$A^a, A^{2a}, A^{3a}, \dots, A^{a^\alpha-a}.$$

Ihre Summe ist

$$(A + A^2 + \dots + A^{a^a-1}) - (A^a + A^{2a} + \dots + A^{a^a-a})$$

oder, was dasselbe ist,

$$(1 + A + A^2 + \dots + A^{a^a-1}) - (1 + A^a + A^{2a} + \dots + A^{a^a-a}),$$

und da die Summe jeder dieser beiden Reihen nach §. 83 durch p teilbar ist, so ist auch die Differenz beider Summen, d. i. die Summe aller zu a^a gehörenden Zahlen $\equiv 0 \pmod{p}$.

Wir haben oben für die Summe aller zum Exponenten $d = a^a b^b \dots$ gehörenden Zahlen das Produkt

$$(A_1 + A_2 + \dots)(B_1 + B_2 + \dots) \dots$$

erhalten, dessen einzelne Faktoren den Faktoren von d , nämlich $a^a, b^b, \dots$ entsprechen. Weiter haben wir gezeigt, daß, wenn d einen seiner Primfaktoren, etwa a , in einer höheren als der ersten Potenz enthält (wenn also d durch eine Quadratzahl a^2 teilbar ist), der entsprechende Faktor

$$A_1 + A_2 + \dots \equiv 0 \pmod{p} \text{ ist.}$$

In diesem Falle ist dann auch das ganze Produkt, d. i. die Summe aller zum Exponenten d gehörenden Zahlen, $\equiv 0 \pmod{p}$. Wenn dagegen d jeden seiner Primfaktoren nur in der ersten Potenz enthält, so ist, wie wir bewiesen haben, jeder Faktor jenes Produkts

$$\equiv -1 \pmod{p}.$$

Das Produkt selbst oder die Summe aller zum Exponenten d gehörenden Zahlen ist dann also

$$\equiv +1 \text{ oder } \equiv -1 \pmod{p},$$

je nachdem die Anzahl der ungeraden Primfaktoren $a, b, c, \dots$ von d gerade oder ungerade ist.

Der vorstehende Satz gilt für jeden Divisor d von $p-1$, also auch für $p-1$ selbst. Wir erhalten so den

Zusatz. Die Summe aller primitiven Wurzeln einer Primzahl p ist $\equiv 0 \pmod{p}$, wenn $p-1$ durch eine Quadratzahl teilbar ist. Sie ist

$$\equiv \pm 1 \pmod{p},$$

wenn die Zahl $p-1$ jeden ihrer Primfaktoren nur in der ersten Potenz enthält, und zwar ist das obere

oder untere Zeichen zu nehmen, je nachdem die Anzahl dieser ungleichen Primfaktoren von $p - 1$ gerade oder ungerade ist.

Beispiele. I. Nach der Tabelle des §. 82, in der $p = 37$ ist, gehören

zum Exponenten	die Zahlen						Summe der- selben
1	1						1
2	36						$36 \equiv -1$
3	10	26					$36 \equiv -1$
4	6	31					$37 \equiv 0$
6	11	27					$38 \equiv +1$
9	7	9	12	16	33	34	$111 \equiv 0$
12	8	14	23	29			$74 \equiv 0$
18	3	4	21	25	28	30	$111 \equiv 0$
36	{ 2	5	13	15	17	18	{ $222 \equiv 0$.
	19	20	22	24	32	35	

II.

$$p = 43.$$

Zum Exponenten	gehören die Zahlen						Summe der- selben
1	1						1
2	42						$42 \equiv -1$
3	6	36					$42 \equiv -1$
6	7	37					$44 \equiv +1$
7	4	11	16	21	35	41	$128 \equiv -1$
14	2	8	22	27	32	39	$190 \equiv +1$
21	{ 9	10	13	14	15	17	{ $259 \equiv +1$
	23	24	25	31	38	40	
42	{ 3	5	12	18	19	20	{ $257 \equiv -1$.
	26	28	29	30	33	34	

§. 86.

Aufgaben.

I. Für welche Werte von p und a ist die Kongruenz $x^3 \equiv a \pmod{p}$ möglich, und für welche nicht?

Lösung. Wenn die Kongruenz

$$(1) \quad x^3 \equiv a \pmod{p}$$

bestehen soll, so muß

$$(2) \quad 3 \text{ Ind. } x \equiv \text{Ind. } a \pmod{\overline{p-1}}$$

sein. Diese Kongruenz ist immer (für jeden Wert von a) möglich, wenn 3 prim zu $p-1$, also p von der Form $6n-1$ ist. Sie hat dann eine einzige Wurzel Ind. x , und somit hat auch die Kongruenz (1) in diesem Falle stets eine, aber auch nur eine Lösung.

Wenn dagegen p die Form $6n+1$ hat, so ist (2) und daher (1) nur möglich, wenn der Index von a durch 3 teilbar ist. Für jedes solche a besitzt (2) drei Lösungen, die mod. $(p-1)$ inkongruent sind, also (1) drei mod. p inkongruente Lösungen.

II. Beweise, daß für jede primitive Wurzel g

$$\text{Ind. } (p-1) \equiv \frac{p-1}{2} \pmod{\overline{p-1}}$$

ist.

Nach dem Fermatschen Satze ist

$$g^{p-1} \equiv 1 \pmod{p},$$

also

$$g^{p-1} - 1 = \left[g^{\frac{1}{2}(p-1)} - 1 \right] \left[g^{\frac{1}{2}(p-1)} + 1 \right]$$

durch p teilbar, und da p eine Primzahl ist, so muß dieselbe entweder in den ersten oder in den zweiten Faktor der rechten Seite aufgehen. Ginge p in den ersten Faktor auf, wäre also

$$g^{\frac{1}{2}(p-1)} - 1 \equiv 0 \pmod{p},$$

so würde g der Voraussetzung zuwider zum Exponenten

$$\frac{p-1}{2}$$

gehören. Daher kann nur

$$g^{\frac{1}{2}(p-1)} + 1 \equiv 0 \pmod{p}$$

sein, und daraus folgt

$$g^{\frac{1}{2}(p-1)} \equiv -1 \equiv p-1 \pmod{p},$$

d. h.

$$\text{Ind. } (p-1) \equiv \frac{1}{2}(p-1) \pmod{\overline{p-1}}.$$

III. Wenn der Exponent n , zu welchem eine Zahl a für den Modul p gehört, ungerade ist, so ist die Kongruenz

$$a^x + 1 \equiv 0 \pmod{p}$$

unmöglich (Fermat, *Varia Opera math.*, S. 163 = *Oeuvres*, Bd. II, S. 209).

Nach §. 82 haben, wenn a zum Exponenten n gehört, Ind. a und $p - 1$ den größten gemeinschaftlichen Divisor $\frac{p-1}{n}$. Wir können also

$$p - 1 = n \cdot \frac{p-1}{n} \quad \text{und} \quad \text{Ind. } a = k \cdot \frac{p-1}{n}$$

setzen, wo k prim zu n ist. Nun folgt aus

$$a^x + 1 \equiv 0 \pmod{p},$$

dafs

$$a^x \equiv p - 1 \pmod{p},$$

also

$$x \text{ Ind. } a \equiv \frac{p-1}{2} \pmod{\frac{p-1}{n}},$$

d. h.

$$x \cdot k \cdot \frac{p-1}{n} \equiv \frac{n}{2} \cdot \frac{p-1}{n} \pmod{n \cdot \frac{p-1}{n}}$$

oder

$$kx \equiv \frac{n}{2} \pmod{n}$$

sein mufs. Das ist nur möglich, wenn $\frac{n}{2}$ eine ganze, also n eine gerade Zahl ist. Unter dieser Bedingung ist die Kongruenz überdies, da k prim zum Modul n ist, stets möglich.

IV. Wenn die ganze Zahl q kein Vielfaches von $p - 1$ ist, so ist

$$S_q = 1^q + 2^q + 3^q + \dots + (p-1)^q \equiv 0 \pmod{p}.$$

Es sei g eine beliebige primitive Wurzel von p . Da dann die Zahlen

$$1, \quad 2, \quad 3, \quad \dots, \quad (p-1)$$

in irgend einer Reihenfolge mit den Resten der Potenzen

$$g, \quad g^2, \quad \dots, \quad g^{p-1}$$

übereinstimmen, so ist

$$S^q \equiv g^q + g^{2q} + g^{3q} + \dots + g^{(p-1)q} \equiv g^q \cdot \frac{g^{(p-1)q} - 1}{g^q - 1} \pmod{p}.$$

Nun ist q kein Vielfaches von $p - 1$, also der mod. p genommene Rest von g^q von 1 verschieden. Daher kann der nach dem Fermatschen Satze in $g^{(p-1)q} - 1$ enthaltene Faktor p bei der Division durch $g^q - 1$ nicht wegfallen, und so ist

$$S_q \equiv 0 \pmod{p}.$$

V. Wenn die Zahl a zu einem durch 4 teilbaren Exponenten $d = 4\delta$ gehört, so gehört auch $p - a$ zu dem Exponenten 4δ .

Aus

$$(p - a)^k \equiv (-1)^k a^k \pmod{p}$$

folgt nämlich für $k = 2\delta$

$$(p - a)^{2\delta} \equiv a^{2\delta} \pmod{p}.$$

Wenn nun a zum Exponenten 4δ gehört, so ist $a^{2\delta} \equiv -1$, folglich auch $(p - a)^{2\delta} \equiv -1$ und erst $(p - a)^{4\delta} \equiv +1$, d. h. $p - a$ gehört zum Exponenten 4δ .

VI. Wenn g eine primitive Wurzel der Primzahl $p = 4n + 1$ ist, so ist auch $p - g$ primitive Wurzel. Für $p = 4n + 3$ dagegen gehört, wenn p primitive Wurzel ist, $p - g$ zum Exponenten $\frac{p-1}{2}$.

Der Beweis ist mit Hülfe von V zu führen. Der Satz ist auf seine Richtigkeit mittels der Tabellen des §. 85 zu prüfen.

VII. Eine aus lauter Neunen gebildete Zahl zu finden, welche durch 41 teilbar ist.

Es soll $10^x - 1$ durch 41 teilbar, oder

$$10^x \equiv 1 \pmod{41}$$

sein. Daraus folgt

$$8x \equiv 0 \pmod{40},$$

$$x \equiv 0 \pmod{5}.$$

Es ist also $x = 5k$, wo k jede ganze Zahl sein kann. Der kleinste Wert von x ist 5; diesem entspricht die Zahl 99999.

Andere Lösung: Da 10 für den Modul 41 zum Exponenten 5 gehört, so ist

$$10^5 - 1 = 99999$$

die kleinste durch 41 teilbare Zahl, die aus lauter Neunen gebildet ist. Allgemein ist $10^{5k} - 1$ für jeden Wert von k durch 41 teilbar.

Übrigens hätte sich die Aufgabe auch durch Division mit 41 in 999... lösen lassen

VIII. Für jede Primzahl p ist die Zahl

$$\frac{(p-1)(p-2)\dots(p-m)}{1.2\dots m} \equiv +1 \text{ oder } \equiv -1 \pmod{p},$$

je nachdem m gerade oder ungerade ist.

Setzt man

$$\frac{(p-1)(p-2)\dots(p-m)}{1.2\dots m} = k,$$

so ist

$$(p-1)(p-2)\dots(p-m) = 1.2\dots m.k$$

oder

$$p^m - \alpha_1 p^{m-1} + \alpha_2 p^{m-2} - \dots \pm 1.2.3\dots m = 1.2\dots m.k,$$

wo $\alpha_1, \alpha_2, \dots$ ganze Zahlen sind und das obere oder untere Zeichen zu nehmen ist, je nachdem m gerade oder ungerade ist. Daraus folgt

$$p^m - \alpha_1 p^{m-1} + \alpha_2 p^{m-2} - \dots \mp \alpha_{m-1} p = (k \mp 1).1.2\dots m.$$

Da die linke Seite durch p teilbar ist, so muß es auch die rechte sein. Jede der Zahlen $1, 2, \dots, m$ ist aber $< p$. Folglich ist bei geradem m die Zahl $k-1$, bei ungeradem m dagegen $k+1$ durch p teilbar.

IX. Wenn a und b zwei durch die Primzahl p nicht teilbare ganze Zahlen bezeichnen, so ist $a^{p-1} - b^{p-1}$ durch p teilbar. So z. B. ist $3^{10} - 2^{10} = 59049 - 1024 = 58025$ ein Vielfaches von 11.

Siebentes Kapitel.

Potenzreste für zusammengesetzte Moduln.

§. 87.

Der Exponent, zu welchem eine Zahl für einen Modul gehört.

Es seien a und m relative Primzahlen. Wir betrachten die Reihe der Potenzen von a

$$1, a, a^2, \dots, a^m, \dots$$

und denken uns jede derselben durch ihren kleinsten positiven Rest für den Modul m ersetzt. Unter diesen Resten kann sich weder Null noch eine Zahl befinden, die mit m einen Faktor gemeinschaftlich hätte; denn da a prim zu m ist, so ist es auch jede Potenz von a . Die Reihe der Potenzreste von a kann also keine anderen Zahlen als diejenigen enthalten, welche prim zu m und nicht gröfser als m sind. Damit ist aber nicht gesagt, dafs sie auch alle diese Zahlen wirklich enthalten mufs, dafs nicht einige derselben fehlen können. Wir sehen somit, dafs die Anzahl der Potenzreste höchstens $\varphi(m)$ beträgt, und da $\varphi(m) < m$ ist, so müssen unter den m ersten Gliedern der Reihe $1, a, a^2, \dots$ mindestens zwei Glieder vorhanden sein, welche für den Modul m denselben Rest liefern. Es sei $a^k \equiv a^{k'} \pmod{m}$, und es werde $k > k'$ vorausgesetzt. Dann folgt durch die Division mit $a^{k'}$, deren Zulässigkeit aus §. 34 erhellt,

$$a^{k-k'} \equiv 1 \pmod{m},$$

und da jede der Zahlen k, k' kleiner als m ist, so ist auch $k - k' < m$. Es giebt somit zwischen 1 und a^m wenigstens ein

Glied in der Reihe $1, a, a^2, \dots, a^m, \dots$, welches für den Modul m den Rest 1 liefert.

Möglicherweise sind mehrere Potenzen dieser Art zwischen 1 und a^m vorhanden. Den Exponenten der niedrigsten Potenz von a , welche für den Modul m den Rest 1 giebt, nennt man auch hier den Exponenten, zu welchem a für den Modul m gehört, und man erkennt wie im Falle eines Primzahlmoduls, dafs, wenn n dieser Exponent ist, die Reste der Potenzen

$$1, a, a^2, \dots, a^{n-1}, a^n, \dots$$

eine periodische Reihe bilden, indem die Reste der n ersten Glieder, die sämtlich inkongruent sind, und die man die Periode von a für den Modul m nennt, sich in unveränderter Folge wiederholen.

Beispiele. I. Die Zahl 3 gehört für den Modul 40 zum Exponenten 4; ihre Periode ist 3, 9, 27, 1.

II. Die Zahl 5 gehört für den Modul 49 zum Exponenten 42; ihre Periode ist

5, 25, 27, 37, 38, 43, 19, 46, 34, 23, 17, 36, 33, 18, 41, 9, 45, 29, 47, 39, 48, 44, 24, 22, 12, 11, 6, 30, 3, 15, 26, 32, 13, 16, 31, 8, 40, 4, 20, 2, 10, 1.

§. 88.

Der verallgemeinerte Fermatsche Satz. (Euler, *Commentationes arithmet. coll. I*, p. 274 ff.)

Wenn eine Zahl a prim zum Modul ist und $\varphi(m)$ wieder die Anzahl der Zahlen bezeichnet, die prim zu m und nicht gröfser als m sind, so ist

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Beweis. Wenn wir jede der $\varphi(m)$ Zahlen

$$(1) \quad \alpha, \beta, \gamma, \delta, \dots,$$

die prim zu m und kleiner als m sind, mit a multiplizieren, so erhalten wir die $\varphi(m)$ Produkte

$$(2) \quad a\alpha, a\beta, a\gamma, a\delta, \dots,$$

die für den Modul m sämtlich verschiedene Reste geben werden. Hätte man nämlich

$$a\alpha \equiv a\beta \pmod{m},$$

wo α und β zwei beliebige, aber voneinander verschiedene Zahlen der Reihe (1) sein mögen, so würde die nach §. 34 zulässige Division mit a

$$\alpha \equiv \beta \pmod{m}$$

liefern, und das widerspricht der Annahme, die wir in Betreff der Zahlen α, β gemacht haben. Da somit die Produkte (2) für den Modul m inkongruent sind, und da außerdem jedes derselben offenbar prim zu m ist, so müssen ihre kleinsten positiven Reste — abgesehen von der Reihenfolge — mit den Zahlen (1) übereinstimmen. Es muß somit das Produkt der Zahlen (2) dem Produkt der Zahlen (1) kongruent, also

$$a^{\varphi(m)} \cdot \alpha \cdot \beta \cdot \gamma \cdot \delta \dots \equiv \alpha \cdot \beta \cdot \gamma \cdot \delta \dots \pmod{m}$$

sein. Hieraus folgt durch Division mit $\alpha\beta\gamma\delta\dots$

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Weiter ergeben sich die beiden leicht zu beweisenden Sätze:

Zusatz I. Der Exponent, zu welchem eine Zahl, die prim zum Modul m ist, für diesen Modul gehört, ist ein Divisor von $\varphi(m)$.

Zusatz II. Wenn es eine Zahl giebt, die für den Modul m zum Exponenten $m - 1$ gehört, so ist m eine Primzahl.

Anwendungen. I. Es soll gezeigt werden, daß

$$m = 2^{16} + 1 = 65537$$

eine Primzahl ist.

Es sei $a = 3$. Die Divisoren von $m - 1 = 2^{16}$ sind

$$1, 2, 2^2, 2^3, \dots, 2^{16}.$$

Nun ergibt sich mod. 65537

$$3^1 \equiv 3, \quad 3^2 \equiv 9, \quad 3^{2^2} \equiv 81, \quad 3^{2^3} \equiv 81^2 \equiv 6561,$$

$$3^{2^4} \equiv 6561^2 \equiv 43046721 \equiv -11088,$$

$$3^{2^5} \equiv (-11088)^2 \equiv 122943744 \equiv -3668,$$

.....

So fortfahrend überzeugt man sich, daß erst

$$3^{2^{16}} \equiv 1 \pmod{65537}$$

ist. $2^{16} + 1$ ist also in der That eine Primzahl.

Anmerkung. Zur Ausführung der erforderlichen Quadrierungen bedient man sich mit Vorteil der „Tafel der Viertelquadrate aller ganzen Zahlen von 1 bis 200 000 von Joseph Bilater. Wien, 1887“. Vergl. übrigens §. 8, Anmerkung II.

II. Auflösung der Kongruenz ersten Grades mit einer Unbekannten (vergl. §. 45). — Um die Kongruenz

$$ax \equiv b \pmod{m}$$

zu lösen, multiplizieren wir beiderseits mit $a^{\varphi(m)-1}$ und erhalten

$$a^{\varphi(m)} x \equiv b \cdot a^{-1 + \varphi(m)} \pmod{m}$$

oder, da

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

ist,

$$x \equiv b \cdot a^{-1 + \varphi(m)} \pmod{m}.$$

Beispiel. Es soll die Kongruenz $12x \equiv 13 \pmod{25}$ gelöst werden. Da $\varphi(25) = 20$ ist, so haben wir beide Seiten mit $12^{19} \equiv -2 \pmod{25}$ zu multiplizieren. Wir erhalten

$$12^{20} \cdot x, \text{ d. i. } x \equiv -26 \equiv 24 \pmod{25}.$$

Anmerkung. Wenn man weiß, daß die Zahl a für den Modul m zum Exponenten $d < \varphi(m)$ gehört, so genügt schon eine Multiplikation mit a^{d-1} .

Beispiel.

$$13x \equiv 5 \pmod{28}.$$

Da

$$13^2 = 169 \equiv 1 \pmod{28}$$

ist, so ist $d = 2$, und wir erhalten, wenn wir beide Seiten der Kongruenz mit $13^{2-1} = 13$ multiplizieren,

$$x \equiv 5 \cdot 13 \equiv 65 \equiv 9 \pmod{28}.$$

§. 89.

Verteilung der Zahlen, die prim zu m sind, unter die Divisoren von $\varphi(m)$ als Exponenten.

Lehrsatz. Wenn m und n relative Primzahlen sind und eine Zahl a für den Modul m zum Exponenten α , für den Modul n zum Exponenten β gehört, so gehört sie für den Modul mn zum Exponenten $\frac{\alpha\beta}{d}$, wo d den größten gemeinschaftlichen Divisor von α und β bezeichnet.

Beweis. Es sei

$$\alpha = \alpha' d, \quad \beta = \beta' d,$$

wo α', β' prim zu einander sind. Dann ist

$$a^{\alpha' d} \equiv 1 \pmod{m}, \text{ also auch } a^{\alpha' \beta' d} \equiv 1 \pmod{m},$$

und ebenso

$$a^{\beta' d} \equiv 1 \pmod{n}, \text{ also auch } a^{\alpha' \beta' d} \equiv 1 \pmod{n}.$$

Da demnach die Differenz $a^{\alpha' \beta' d} - 1$ durch jede der relativen Primzahlen m, n teilbar ist, so ist sie auch durch das Produkt mn teilbar, d. h. es ist

$$a^{\alpha' \beta' d} = a^{\frac{\alpha \beta}{d}} \equiv 1 \pmod{mn}.$$

Es ist jetzt noch zu beweisen, daß $\alpha' \beta' d$ der kleinste Exponent ist, auf den erhoben a für den Modul mn den Rest 1 liefert. Bezeichnen wir für einen Augenblick den Exponenten, zu welchem a für den Modul mn gehört, mit e , so ist wegen $a^e \equiv 1 \pmod{mn}$ auch $a^e \equiv 1 \pmod{m}$, also e ein Vielfaches von $\alpha' d$. Ebenso ergibt sich, daß e ein Vielfaches von $\beta' d$ sein muß. e ist also ein Vielfaches von $\alpha' \beta' d$, und da e jedenfalls nicht größer als $\alpha' \beta' d$ sein darf, so ist

$$e = \alpha' \beta' d = \frac{\alpha \beta}{d}.$$

Beispiel. Da die Zahl 3 für den Modul 5 zum Exponenten 4 und für den Modul 7 zum Exponenten 6 gehört, so gehört sie für den Modul 35 zum Exponenten

$$\frac{4 \cdot 6}{2} = 12.$$

Der vorhergehende Satz ermöglicht es, die Verteilung der Zahlen, die prim zu m und nicht größer als m sind, unter die Divisoren von $\varphi(m)$ auszuführen, sobald die Verteilung für die in m enthaltenen Primzahlen als Moduln gegeben ist, ohne daß man nötig hätte, die Reihe der Potenzreste jeder einzelnen in Betracht kommenden Zahl (bis zum Reste 1) zu berechnen.

Aufgabe. Die Zahlen zu ermitteln, welche für den Modul 55 zum Exponenten 10 gehören.

Hülftabellen:

Modul 5.		Modul 11.	
Exponent	Zugehörige Zahlen	Exponent	Zugehörige Zahlen
1	1	1	1
2	4	2	10
4	2, 3.	5	3, 4, 5, 9
		10	2, 6, 7, 8.

Lösung. Da 10 das kleinste Vielfache von 1 und 10, sowie von 2 und 5, endlich von 2 und 10 ist, so gehören zum Exponenten 10 für den Modul 55

erstens die Zahlen, welche für 5 zum Exponenten 1 und zugleich für 11 zum Exponenten 10 gehören,
zweitens die Zahlen, welche für 5 zum Exponenten 2 und zugleich für 11 zum Exponenten 5 gehören,
drittens die Zahlen, welche für 5 zum Exponenten 2 und zugleich für 11 zum Exponenten 10 gehören.

Für den Modul 5 gehören unterhalb 55 zum Exponenten 1

(I) 1, 6, 16, 21, 26, 31, 36, 41, 46, 51.

[Die Zahl 11 mußte weggelassen werden, da sie nicht prim zum Modul 55 ist.]

Für den Modul 11 gehören unterhalb 55 zum Exponenten 10

(II) $\left\{ \begin{array}{l} 2, 13, 24, 46; \quad 6, 17, 28, 39; \\ 7, 18, 29, 51; \quad 8, 19, 41, 52. \end{array} \right.$

[Die Zahlen 35, 50, 40, 30 mußten weggelassen werden, da sie nicht prim zum Modul 55 sind.]

Zum Exponenten 10 für den Modul 55 gehören also **erstens** die Zahlen, welche sich zugleich in (I) und (II) vorfinden, nämlich 6, 41, 46, 51.

Für den Modul 5 gehören zum Exponenten 2

(III) 4, 9, 14, 19, 24, 29, 34, 39, 49, 54.

Für den Modul 11 gehören zum Exponenten 5

(IV) $\left\{ \begin{array}{l} 3, 14, 36, 47; \quad 4, 26, 37, 48; \\ 16, 27, 38, 49; \quad 9, 31, 42, 53. \end{array} \right.$

Also gehören für den Modul 55 zum Exponenten 10 **zweitens** die Zahlen 4, 9, 14, 49.

Für den Modul 5 gehören zum Exponenten 2 die Zahlen (III), für den Modul 11 zum Exponenten 10 die Zahlen (II), also für den Modul 55 zum Exponenten 10 drittens die Zahlen 19, 24, 29, 39.

Die gesuchten Zahlen sind also, der Größe nach geordnet.

4, 6, 9, 14, 19, 24, 29, 39, 41, 46, 49, 51.

Anmerkung. $\varphi(55) = 40$ hat die acht Divisoren

1, 2, 4, 5, 8, 10, 20, 40.

Da nun das kleinste Vielfache je einer der Zahlen 1, 2, 4 mit einer der Zahlen 1, 2, 5, 10 weder 8 noch 40 sein kann, so sehen wir, daß es keine Zahl giebt, welche für den Modul 55 zum Exponenten 8 oder zum Exponenten 40 gehört. Wie sich die 40 Zahlen, die prim zu 55 und nicht größer als 55 sind, unter die Divisoren von 40 als Exponenten verteilen, ist aus der folgenden Tabelle ersichtlich.

Modul 55, $\varphi(55) = 40$.

Exponent	Zugehörige Zahlen							
1	1							
2	21	34	54					
4	12	23	32	43				
5	16	26	31	36				
8	nicht vorhanden							
10	4	6	9	14	19	24		
	29	39	41	46	49	51		
20	2	8	7	8	13	17	18	27
	28	37	33	42	47	48	52	53
40	nicht vorhanden.							

Für den Modul 50 ergiebt sich ebenso die Tabelle:

Exponent	Zugehörige Zahlen							
1	1							
2	49							
4	7	43						
5	11	21	31	41				
10	9	19	29	39				
20	3	13	17	23	27	33	37	47.

In §. 73 haben wir bewiesen, daß im Falle eines Primzahlmoduls p zu jedem Divisor d von $\varphi(p) = p - 1$ als Exponenten $\varphi(d)$ Zahlen gehören. Die vorstehenden Beispiele zeigen, daß dieser Satz für zusammengesetzte Moduln im allgemeinen nicht besteht. Für $m = 50$ gilt er, für $m = 55$ nicht.

Wir nennen auch hier eine Zahl, welche für den Modul m zum Exponenten $\varphi(m)$ gehört, eine primitive Wurzel von m . Die Zahl 50 hat also primitive Wurzeln, d. h. zum Exponenten $\varphi(50) = 20$ gehörende Zahlen, und zwar

$$\varphi(20) = \varphi \varphi(50) = 8$$

solche Zahlen. Für $m = 55$ sind aber Zahlen, die zum Exponenten $\varphi(55) = 40$ gehören, nicht vorhanden, oder 55 besitzt keine primitiven Wurzeln. Es fragt sich jetzt, welche zusammengesetzten Zahlen primitive Wurzeln besitzen und welche nicht.

§. 90.

Zahlen, welche keine primitiven Wurzeln besitzen können.

Es sei

$$m = 2^k p^\lambda q^\mu \dots,$$

wo $k, \lambda, \mu, \dots$ ganze positive Zahlen, $p, q, \dots$ voneinander verschiedene ungerade Primzahlen bezeichnen. Wenn nun eine Zahl a prim zu m ist, so ist sie auch prim zu jedem der Faktoren $2^k, p^\lambda, q^\mu, \dots$ von m , und dann ist nach dem verallgemeinerten Fermatschen Satze

$$a^{\varphi(2^k)} \equiv 1 \pmod{2^k}, \quad a^{\varphi(p^\lambda)} \equiv 1 \pmod{p^\lambda}, \quad \dots$$

Bezeichnet daher M das kleinste Vielfache der Exponenten dieser Kongruenzen, so ist auch

$$a^M \equiv 1 \pmod{2^k}, \quad a^M \equiv 1 \pmod{p^\lambda}, \quad a^M \equiv 1 \pmod{q^\mu}, \quad \dots,$$

die Differenz $a^M - 1$ ist somit durch jeden der Moduln teilbar, und da diese prim zu einander sind, so muß $a^M - 1$ auch durch das Produkt derselben teilbar sein, d. h. es ist

$$a^M \equiv 1 \pmod{m}.$$

Der Exponent, zu welchem a für den Modul m gehört, ist also entweder das kleinste Vielfache der Zahlen

$$\varphi(2^k), \varphi(p^2), \varphi(q^u), \dots$$

oder ein Divisor dieses Vielfachen.

Nun ist a eine primitive Wurzel von m , wenn es zum Exponenten

$$\varphi(m) = \varphi(2^k) \varphi(p^2) \varphi(q^u) \dots$$

gehört, und dies kann nur der Fall sein, wenn das kleinste Vielfache der Zahlen

$$\varphi(2^k), \varphi(p^2), \varphi(q^u), \dots$$

gleich dem Produkt dieser Zahlen ist, wenn also letztere prim zu einander sind. Offenbar ist aber jede der Zahlen

$$\varphi(p^2) = (p-1)p^{2-1}, \quad \varphi(q^u) = (q-1)q^{u-1}, \dots$$

gerade, und auch

$$\varphi(2^k) = 2^{k-1}$$

ist eine gerade Zahl, wenn $k > 1$ ist. Daher haben diese Zahlen jedenfalls den Faktor 2 gemeinschaftlich, ihr kleinstes Vielfache ist also kleiner als ihr Produkt, wenn

erstens m mehr als eine ungerade Primzahl enthält;

zweitens m zwar nur eine ungerade Primzahl, aber eine höhere als die erste Potenz von 2 enthält.

In diesen beiden Fällen kann es also keine primitive Wurzel geben.

Es bleibt jetzt noch der Fall zu untersuchen, in welchem der Modul überhaupt keine ungerade Primzahl enthält, sondern gleich 2^k ist, für welchen Wert von m man nach dem Früheren

$$\varphi(m) = 2^{k-1}$$

hat. Da die Zahl a prim zum Modul vorausgesetzt wird, so muß sie in diesem Falle ungerade, also von einer der beiden Formen $4n \pm 1$ sein, und wir erhalten

$$a = \pm 1 + 4n,$$

$$a^2 = 1 + 8n_1,$$

$$a^{2^2} = 1 + 16n_2,$$

$$a^{2^3} = 1 + 32n_3,$$

$$\dots \dots \dots$$

$$a^{2^{k-2}} = 1 + 2^k n_{k-2},$$

wo $n, n_1, n_2, \dots, n_{k-2}$ ganze Zahlen bedeuten. Wenn nun $k > 2$ ist, so ist die letzte Gleichung gleichbedeutend mit der Kongruenz

$$a^{2^k-2}, \text{ d. i. } a^{\frac{1}{2} \varphi(2^k)} \equiv 1 \pmod{2^k},$$

a gehört danach zu einem Exponenten, der kleiner als $\varphi(2^k)$ ist, und somit giebt es drittens keine primitive Wurzel, wenn der Modul eine höhere als die zweite Potenz von 2 ist.

Primitive Wurzeln können also nur vorhanden sein, wenn der Modul

- erstens eine Potenz einer ungeraden Primzahl, oder
- zweitens das Doppelte einer Potenz einer ungeraden Primzahl, oder
- drittens gleich 4 ist.

Wir wollen jetzt zeigen, daß es in den beiden ersten Fällen (der dritte Fall wird später besonders betrachtet werden) auch thatsächlich primitive Wurzeln giebt, und wollen untersuchen, wieviele es sind, wie man sie bestimmt, und welche Anwendungen sie finden.

§. 91.

Primitive Wurzeln einer Potenz einer ungeraden Primzahl.

Lehrsatz I. Wenn eine Zahl primitive Wurzel von p^2 ist, so muß sie auch primitive Wurzel von p sein.

Beweis. Angenommen, die Zahl a sei eine primitive Wurzel von p^2 , gehöre also für den Modul p^2 zum Exponenten $(p-1)p^{2-1}$, sie sei aber keine primitive Wurzel von p , sondern gehöre für den Modul p zum Exponenten d . Dann muß d ein eigentlicher Divisor von $p-1$ sein, und es ist

$$a^d \equiv 1 \pmod{p}$$

oder

$$a^d = 1 + kp,$$

wo k eine ganze Zahl bezeichnet. Wird diese Gleichung auf die p^2 Potenz erhoben, so giebt sich

$$a^{d^2} = 1 + \frac{p}{1} kp + \frac{p(p-1)}{1 \cdot 2} k^2 p^2 + \dots$$

oder

$$a^{d^2} = 1 + k_1 p^2,$$

wo k_1 eine ganze Zahl bezeichnet, auf deren Gröfse es hier nicht ankommt. Ebenso erhält man durch nochmalige Erhebung auf die p^2 Potenz

$$a^{d p^2} = 1 + \frac{p}{1} k_1 p^2 + \frac{p(p-1)}{1 \cdot 2} k_1^2 p^4 + \dots$$

oder

$$a^{d p^2} = 1 + k_2 p^2,$$

weiter

$$a^{d p^3} = 1 + k_3 p^4,$$

$$\dots \dots \dots$$

$$a^{d p^{\lambda-1}} = 1 + k_{\lambda-1} p^{\lambda};$$

darin bezeichnen

$$k_2, k_3, \dots, k_{\lambda-1}$$

ebenfalls ganze Zahlen. Die letzte Gleichung ist gleichbedeutend mit der Kongruenz

$$a^{d p^{\lambda-1}} \equiv 1 \pmod{p^{\lambda}}.$$

Da nun a für den Modul p^{λ} zum Exponenten $(p-1)p^{\lambda-1}$ gehört, so erfordert diese Kongruenz, daß $d p^{\lambda-1}$ ein Vielfaches von $(p-1)p^{\lambda-1}$, also d ein Vielfaches von $p-1$ sei. Das ist aber unmöglich, da d ein eigentlicher Divisor von $p-1$, also $< p-1$ ist. Somit muß jede Zahl a , die eine primitive Wurzel von p^{λ} ist, auch eine primitive Wurzel von p sein. Wenn also p^{λ} überhaupt primitive Wurzeln besitzt, so sind sie unter den primitiven Wurzeln von p zu suchen.

Lehrsatz II. Jede primitive Wurzel a von p , für welche $a^{p-1} - 1$ nicht durch p^2 teilbar ist, ist auch eine primitive Wurzel von p^{λ} .

Beweis. Es sei d der Exponent der höchsten Potenz von p , welche in $a^{p-1} - 1$ aufgeht, also

$$a^{p-1} - 1 = k p^d,$$

wo k eine ganze Zahl bezeichnet. Dann ist

$$a^{p-1} = 1 + k p^d,$$

und hieraus erhält man, wie im Beweise des vorhergehenden Satzes,

$$a^{(p-1)p} = 1 + k_1 p^{d+1},$$

$$a^{(p-1)p^2} = 1 + k_2 p^{d+2},$$

$$\dots \dots \dots$$

$$a^{(p-1)p^{\lambda-d}} = 1 + k_{\lambda-d} p^{\lambda},$$

wo $k_1, k_2, \dots$ ganze Zahlen bezeichnen. Die letzte Gleichung ist gleichbedeutend mit der Kongruenz

$$a^{(p-1)p^{\lambda-d}} \equiv 1 \pmod{p^{\lambda}}.$$

Soll nun a eine primitive Wurzel von p^{λ} sein, also zum Exponenten $(p-1)p^{\lambda-1}$ gehören, so ist $d = 1$ anzunehmen. Wenn dagegen $d > 1$ ist, so gehört a für den Modul p^{λ} zu einem Exponenten, der kleiner als $(p-1)p^{\lambda-1}$ ist, a ist dann also keine primitive Wurzel von p^{λ} . Die Zahl a , von der wir voraussetzen, daß sie eine primitive Wurzel von p sei, ist also stets, aber auch nur dann eine primitive Wurzel von p^{λ} , wenn die nach dem Fermatschen Satze durch p teilbare Zahl $a^{p-1} - 1$ nicht durch p^2 teilbar ist.

Beispiele. 3 ist primitive Wurzel von 7, 17, 31. Da nun $3^6 - 1 = 728$ nicht durch 49, $3^{16} - 1 = 43\,046\,720$ nicht durch 289 und $3^{30} - 1 = 205\,891\,132\,094\,648$ nicht durch 961 teilbar ist, so ist 3 für jeden Wert von λ auch primitive Wurzel der Potenzen $7^{\lambda}, 17^{\lambda}, 31^{\lambda}$.

Lehrsatz III. Die Zahl p^{λ} besitzt

$$\varphi \varphi(p^{\lambda}) = \varphi[(p-1)p^{\lambda-1}] = (p-1)p^{\lambda-2} \varphi(p-1)$$

primitive Wurzeln.

Beweis. Die Primzahl p besitzt nach §. 75 $\varphi(p-1)$ primitive Wurzeln. Eine derselben sei g . Dann ist die Zahl

$$a = g + kp$$

auch eine primitive Wurzel von p^{λ} , wenn k so gewählt wird, daß $a^{p-1} - 1$ nicht durch p^2 teilbar sei. Es ist aber

$$\begin{aligned} a^{p-1} - 1 &= (g + kp)^{p-1} - 1 = (g^{p-1} - 1) \\ &+ \frac{p-1}{1} g^{p-2} kp + \frac{(p-1)(p-2)}{1 \cdot 2} g^{p-3} k^2 p^2 + \dots, \end{aligned}$$

folglich

$$a^{p-1} - 1 \equiv (g^{p-1} - 1) + \frac{p-1}{1} g^{p-2} kp \pmod{p^2}.$$

Um also a zu einer primitiven Wurzel von p^{λ} zu machen, haben wir über die in a enthaltene noch unbestimmte Zahl k so zu verfügen, daß die rechte Seite der vorhergehenden Kongruenz nicht durch p^2 , also

$$\frac{g^{p-1} - 1}{p} + \frac{p-1}{1} g^{p-2} k$$

nicht durch p teilbar sei.

Es ist dies die Summe zweier Zahlen, und wenn die erste derselben, d. i.

$$\frac{g^{p-1} - 1}{p}$$

durch p teilbar ist, so wird die Summe es nicht sein, wenn die zweite Zahl, d. i.

$$\frac{p-1}{1} g^{p-2} k$$

nicht durch p teilbar ist, oder — da $p-1$ und g prim zu p sind — wenn k kein Vielfaches der Primzahl p ist. Für jeden solchen Wert von k ist $a = g + kp$ eine primitive Wurzel von p^2 , und um alle in diesem Falle vorhandenen primitiven Wurzeln von p^2 zu erhalten, die für diesen Modul inkongruent sind, hat man k die $\varphi(p^2-1)$ Werte zu erteilen, die prim zu p und kleiner als p^2-1 sind.

Wenn dagegen

$$\frac{g^{p-1} - 1}{p}$$

nicht durch p teilbar, sondern $\equiv \alpha \pmod{p}$, also

$$\frac{g^{p-1} - 1}{p} + \frac{p-1}{1} g^{p-2} k \equiv \alpha - g^{p-2} k \pmod{p}$$

ist, so ergibt sich durch Multiplikation mit g wegen $g^{p-1} \equiv 1 \pmod{p}$

$$g \left(\frac{g^{p-1} - 1}{p} + \frac{p-1}{1} g^{p-2} k \right) \equiv \alpha g - k \pmod{p},$$

und da g prim zu p ist, das g fache einer Zahl also durch p teilbar ist oder nicht ist, je nachdem die Zahl selbst es ist oder nicht ist, so erhalten wir das Resultat, daß

$$a = g + kp$$

eine primitive Wurzel von p^2 ist, wenn $\alpha g - k$ für den Modul p einen von Null verschiedenen Rest giebt. Wir bezeichnen diesen Rest mit $-h$; dann ist

$$\alpha g - k \equiv -h, \text{ also } k \equiv \alpha g + h \pmod{p}.$$

Für jede durch p nicht teilbare Zahl h stellt also der Ausdruck

$$a = g + kp = g + (\alpha g + h)p = g(1 + \alpha p) + hp$$

eine primitive Wurzel von p^2 dar. Will man nur die mod. p^2 inkongruenten primitiven Wurzeln von p^2 erhalten, so hat man h nur die $\varphi(p^2-1)$ Werte beizulegen, welche prim zu p und kleiner als p^2-1 sind.

Jede primitive Wurzel g von p liefert also in jedem Falle $\varphi(p^2-1)$ primitive Wurzeln von p^2 .

Wir haben jetzt noch zu zeigen, daß die so erhaltenen primitiven Wurzeln von p^2 für diesen Modul inkongruent sind.

Die Inkongruenz der aus derselben primitiven Wurzel g von p entstandenen primitiven Wurzeln von p^2 geht aus ihrer Bildungsweise ohne weiteres hervor. Es können aber auch zwei primitive Wurzeln von p^2 , die aus verschiedenen primitiven Wurzeln g, g_1 von p herrühren, nicht mod. p^2 kongruent sein; denn wenn

$$g + kp \equiv g_1 + k_1p \pmod{p^2}$$

wäre, so müßte auch

$$g + kp \equiv g_1 + k_1p \pmod{p},$$

folglich

$$g \equiv g_1 \pmod{p}$$

sein, und das widerspricht der Voraussetzung.

Da nun p^2 keine primitive Wurzel besitzt, die nicht auch primitive Wurzel von p wäre, und da jede der $\varphi(p-1)$ primitiven Wurzeln von p uns $\varphi(p^2-1)$ primitive Wurzeln von p^2 liefert, die sämtlich — mögen sie von derselben primitiven Wurzel oder von verschiedenen primitiven Wurzeln von p herrühren — für den Modul p^2 inkongruent sind, so besitzt p^2

$\varphi(p-1) \cdot \varphi(p^2-1) = (p-1)p^{2-2} \varphi(p-1) = \varphi \varphi(p^2)$ primitive Wurzeln.

Aufgabe. Die primitiven Wurzeln von p^2 zu berechnen, wenn diejenigen von p gegeben sind.

Lösung. Man nimmt eine primitive Wurzel g von p , dividiert $g^{p-1} - 1$ durch p und bestimmt den Rest des Quotienten dieser Division für den Modul p . Mag nun dieser Rest, den wir mit α bezeichnen wollen, Null oder von Null verschieden sein, in jedem Falle liefert der Ausdruck

$$a = g(1 + \alpha p) + hp$$

die $\varphi(p^2-1)$ inkongruenten primitiven Wurzeln von p^2 , welche von der primitiven Wurzel g von p herrühren, wenn man h der Reihe nach die $\varphi(p^2-1)$ Werte beilegt, die prim zu p und kleiner

als p^{i-1} sind. Wenn man so mit jeder primitiven Wurzel von p verfährt, so erhält man alle primitiven Wurzeln von p^i .

Beispiele. I. Die Zahl 5 hat die primitiven Wurzeln 2 und 3. Welches sind die primitiven Wurzeln von $5^3 = 125$?

Da

$$\frac{2^4 - 1}{5} = 3$$

und

$$\frac{3^4 - 1}{5} = 16 \equiv 1 \pmod{5}$$

ist, so erhalten wir die primitiven Wurzeln von 125, wenn wir in jedem der beiden Ausdrücke

$$a_1 = 2(1 + 3 \cdot 5) + 5h = 32 + 5h,$$

$$a_2 = 3(1 + 1 \cdot 5) + 5h = 18 + 5h$$

für h die 20 Werte setzen, die prim zu 5 und < 25 sind, also die Werte

1, 2, 3, 4; 6, 7, 8, 9; 11, 12, 13, 14; 16, 17, 18, 19; 21, 22, 23, 24.

Der Ausdruck a_1 liefert also die primitiven Wurzeln

37, 42, 47, 52; 62, 67, 72, 77; 87, 92, 97, 102; 112, 117, 122, 2;
12, 17, 22, 27;

der Ausdruck a_2 liefert

23, 28, 33, 38; 48, 53, 58, 63; 73, 78, 83, 88; 98, 103, 108, 113;
123, 3, 8, 13.

II. Welches sind die primitiven Wurzeln von 121? Die Zahl 11 hat die primitiven Wurzeln 2, 6, 7, 8, und man erhält diejenigen von 121, wenn man in den vier Ausdrücken

$$a_1 = 2(1 + 5 \cdot 11) + 11h = 112 + 11h \equiv -9 + 11h,$$

$$a_2 = 6(1 + 5 \cdot 11) + 11h = 336 + 11h \equiv -27 + 11h,$$

$$a_3 = 7(1 + 2 \cdot 11) + 11h = 161 + 11h \equiv 40 + 11h,$$

$$a_4 = 8(1 + 4 \cdot 11) + 11h = 360 + 11h \equiv -3 + 11h$$

h die Werte

1, 2, 3, 4, 5, 6, 7, 8, 9, 10

beilegt.

§. 92.

Primitive Wurzeln von $2p^2$.

Lehrsatz I. Jede ungerade Zahl gehört für den Modul $2p^2$ zu demselben Exponenten wie für den Modul p^2 .

Beweis. Wir nehmen an, a sei eine ungerade Zahl und gehöre für den Modul p^2 zum Exponenten e , so daß also

$$a^e \equiv 1 \pmod{p^2}$$

ist. Da nun a und folglich auch a^e ungerade ist, so besteht auch die Kongruenz

$$a^e \equiv 1 \pmod{2}.$$

Somit ist $a^e - 1$ sowohl durch p^2 als auch durch 2 teilbar, und da p^2 und 2 relative Primzahlen sind, so muß ihr Produkt in $a^e - 1$ aufgehen, folglich

$$a^e \equiv 1 \pmod{2p^2}$$

sein. e ist somit entweder gleich dem Exponenten, zu welchem a für den Modul $2p^2$ gehört, und den wir e' nennen wollen, oder ein Vielfaches dieses Exponenten.

Andererseits folgt aus der Kongruenz

$$a^{e'} \equiv 1 \pmod{2p^2},$$

daß auch

$$a^{e'} \equiv 1 \pmod{p^2}$$

ist. e' ist somit entweder gleich e oder ein Vielfaches von e . Wir schließen daraus, daß $e = e'$ ist, d. h. daß a für die beiden Moduln p^2 und $2p^2$ zu demselben Exponenten gehört.

Lehrsatz II. Die Zahl $2p^2$ besitzt ebenso viele primitive Wurzeln wie p^2 .

Beweis. Für den Modul p^2 giebt es $\varphi(p^2)$ primitive Wurzeln, die teils ungerade, teils gerade sind. Die ungeraden sind nach dem vorhergehenden Satze auch primitive Wurzeln von $2p^2$. Weiter kann jede gerade primitive Wurzel a von p^2 durch die mod. p^2 ihr kongruente Zahl $a + p^2$ ersetzt werden. Diese letztere ist ebenfalls eine primitive Wurzel von p^2 und, weil sie ungerade ist, auch primitive Wurzel von $2p^2$. Die Moduln p^2 und $2p^2$ besitzen also gleich viele primitive Wurzeln.

Beispiele. Im Falle $m = 27$ ist $p = 3$, $g = 2$,

$$\alpha, \text{ d. i. } \frac{2^3 - 1}{3} = 1,$$

also

$$a = 2(1 + 1.3) + 3h = 8 + 3h,$$

und darin hat man h die sechs Werte 1, 2, 4, 5, 7, 8 beizulegen. Es ergeben sich als primitive Wurzeln von 27 die sechs Zahlen

$$11, 14, 20, 23, 2, 5;$$

folglich hat 54 die sechs primitiven Wurzeln 11, 41, 47, 23, 29, 5.

§. 93.

Verteilung der Zahlen, die prim zu p^2 , resp. $2p^2$ sind, unter die Divisoren von $\varphi(p^2) = \varphi(2p^2) = (p-1)p^{2-1}$ als Exponenten.

Lehrsatz I. Wenn g eine primitive Wurzel von p^2 oder $2p^2$ ist und k mit $(p-1)p^{2-1}$ den größten gemeinschaftlichen Divisor d hat, so gehört g^k sowohl für p^2 als auch für $2p^2$ als Modul zum Exponenten

$$\frac{(p-1)p^{2-1}}{d}.$$

Beweis. Es sei e der Exponent, zu welchem g^k für den in Rede stehenden Modul (p^2 oder $2p^2$) gehört; dann ist $g^{ke} \equiv 1$, und da g der Voraussetzung nach zum Exponenten $(p-1)p^{2-1}$ gehört, so muß ke ein Vielfaches von $(p-1)p^{2-1}$ und $\frac{ke}{d}$ ein Vielfaches von

$$\frac{(p-1)p^{2-1}}{d}$$

sein. $\frac{k}{d}$ ist aber prim zu

$$\frac{(p-1)p^{2-1}}{d},$$

weil d der größte gemeinschaftliche Divisor von k und $(p-1)p^{2-1}$ ist. Somit muß e ein Vielfaches von

$$\frac{(p-1)p^{2-1}}{d}$$

sein, und damit e den kleinsten zulässigen Wert erhalte, ist

$$e = \frac{(p-1)p^{\lambda-1}}{d}$$

anzunehmen. Die Potenz g^k gehört somit zum Exponenten

$$\frac{(p-1)p^{\lambda-1}}{d}.$$

Zusatz. Wenn g eine primitive Wurzel von p^{λ} oder $2p^{\lambda}$ und die Zahl k prim zu $(p-1)p^{\lambda-1}$ ist, so ist auch g^k eine primitive Wurzel von p^{λ} oder $2p^{\lambda}$.

Beweis. Wenn k prim zu $(p-1)p^{\lambda-1}$ ist, so ist $d = 1$. Somit gehört dann g^k zum Exponenten $(p-1)p^{\lambda-1}$.

Lehrsatz II. Zu jedem Divisor d von $(p-1)p^{\lambda-1}$ gehören sowohl für p^{λ} als auch für $2p^{\lambda}$ als Modul $\varphi(d)$ Zahlen.

Beweis. Wir setzen der Kürze wegen

$$\frac{(p-1)p^{\lambda-1}}{d} = \alpha$$

und betrachten die Reihe

$$g^{\alpha}, g^{2\alpha}, g^{3\alpha}, \dots, g^{d\alpha},$$

wo g eine primitive Wurzel von p^{λ} oder $2p^{\lambda}$ bezeichnet. Für jedes Glied $g^{k\alpha}$ dieser Reihe besteht nun zwar die Kongruenz

$$(g^{k\alpha})^d \equiv 1 \pmod{p^{\lambda} \text{ oder } 2p^{\lambda}},$$

da $d\alpha = (p-1)p^{\lambda-1}$ ist, das Glied $g^{k\alpha}$ wird aber nur, wenn k prim zu d ist, zum Exponenten d gehören. Wenn nämlich k und d einen größten gemeinschaftlichen Divisor $\delta > 1$ haben, so ist schon

$$(g^{k\alpha})^{\frac{d}{\delta}} \equiv 1 \pmod{p^{\lambda} \text{ oder } 2p^{\lambda}},$$

da in diesem Falle $\frac{k}{\delta}$ eine ganze Zahl κ und

$$g^{\kappa\alpha d} = g^{\kappa(p-1)p^{\lambda-1}} \equiv 1 \pmod{p^{\lambda} \text{ oder } 2p^{\lambda}}$$

ist.

Nun enthält die Reihe der Exponenten

$$\alpha, 2\alpha, 3\alpha, \dots, d\alpha$$

ebenso viele Glieder, die prim zu d sind, wie die Reihe

$$1, 2, 3, \dots, d,$$

und jedes dieser Glieder liefert eine zum Exponenten d gehörende Zahl. Die so erhaltenen Zahlen sind überdies inkongruent; denn wäre

$$g^k \equiv g^{k'} \pmod{p^2 \text{ oder } 2p^2}$$

und etwa $k > k'$, so könnten wir, da g prim zum Modul ist, durch $g^{k'}$ dividieren und erhielten

$$g^{k-k'} \equiv 1 \pmod{p^2 \text{ oder } 2p^2}.$$

Das ist aber, da $k - k' < d$ und g eine primitive Wurzel von p^2 oder $2p^2$ ist, unmöglich. Zum Exponenten d gehören also in der That $\varphi(d)$ verschiedene Zahlen.

Aufgabe. Die Zahlen, die prim zum Modul p^2 oder $2p^2$ und kleiner als derselbe sind, unter die Divisoren von $(p-1)p^{2-1}$ als Exponenten zu verteilen.

Lösung. Man stelle diese Zahlen als Potenzen einer primitiven Wurzel g des Moduls dar. Dann gehört eine Potenz g^k , deren Exponent k mit $(p-1)p^{2-1}$ den größten gemeinschaftlichen Divisor d hat, zum Exponenten

$$\frac{(p-1)p^{2-1}}{d}.$$

Beispiel. Der Modul sei 25. Die Divisoren von $\varphi(25) = 20$ sind 1, 2, 4, 5, 10, 20. Eine primitive Wurzel von 25 ist 2, und man erhält die Tabelle:

Exponent		Zugehörige Zahlen							
1	2^{20}				1				
2	2^{10}				24				
4	2^5	2^{15}			7	18			
5	2^4	2^8	2^{12}	2^{16}	16	6	21	11	
10	2^2	2^6	2^{14}	2^{18}	4	14	9	19	
20	2^1	2^3	2^7	2^9	2	8	3	12	
	2^{11}	2^{13}	2^{17}	2^{19}	23	17	22	13	

§. 94.

Indizes. — Auflösung der Kongruenz ersten Grades und der binomischen Kongruenz für die Moduln p^2 und $2p^2$.

Wenn g eine primitive Wurzel von p^2 oder $2p^2$ ist, so sind, wie wir gesehen haben, die Reste der Potenzen

$$g, g^2, g^3, \dots, g^{(p-1)p^2-1}$$

sämtlich voneinander verschieden. Da nun ihre Anzahl gleich derjenigen der Zahlen ist, die prim zum Modul und kleiner als derselbe sind, so läßt sich jede dieser Zahlen, folglich überhaupt jede Zahl, die prim zum Modul ist, soweit es sich um die Kongruenz für diesen Modul handelt, durch eine Potenz von g ersetzen. Wenn

$$a \equiv g^n \pmod{p^2 \text{ oder } 2p^2},$$

also auch

$$a \equiv g^{n+(p-1)p^2-1} \pmod{p^2 \text{ oder } 2p^2}$$

ist, so nennt man, wie im Falle eines Primzahlmoduls, n den Index von a und schreibt

$$\text{Ind. } a \equiv n \pmod{(p-1)p^2-1}.$$

Wenn man auch für die Moduln p^2 und $2p^2$ Indizestafeln besitzt (der Anhang enthält dieselben für das Gebiet bis 100), so ist man imstande, mittels derselben sowohl die Kongruenz ersten Grades

$$(1) \quad ax \equiv b \pmod{p^2 \text{ oder } 2p^2},$$

als auch die binomische Kongruenz

$$(2) \quad ax^n \equiv b \pmod{p^2 \text{ oder } 2p^2}$$

aufzulösen. Aus (1) erhält man zunächst

$$\text{Ind. } a + \text{Ind. } x \equiv \text{Ind. } b \pmod{(p-1)p^2-1},$$

ebenso aus (2)

$$\text{Ind. } a + n \cdot \text{Ind. } x \equiv \text{Ind. } b \pmod{(p-1)p^2-1}.$$

Diese Kongruenzen bestimmen $\text{Ind. } x$, und dann liefern die Tafeln den Wert, resp. die Werte von x .

Beispiele. I. Es soll die Kongruenz

$$17x \equiv 5 \pmod{125}$$

gelöst werden. Man sieht sofort, daß x durch 5 teilbar sein muß, daß also $x = 5\xi$ gesetzt werden darf. Dann geht die Kongruenz durch Division mit 5 über in

$$17\xi \equiv 1 \pmod{25},$$

und diese liefert

$$\text{Ind. } 17 + \text{Ind. } \xi \equiv \text{Ind. } 1 \pmod{20},$$

d. i.

$$13 + \text{Ind. } \xi \equiv 0,$$

$$\text{Ind. } \xi \equiv -13 \equiv 7 \pmod{20}.$$

Es ist somit

$$\xi \equiv 3 \pmod{25},$$

also

$$x \equiv 15 \pmod{125}.$$

II. Die Kongruenz

$$53x \equiv 599 \pmod{882 = 9 \cdot 98}$$

lösen wir zunächst für den Modul 9. Wir erhalten der Reihe nach

$$53x \equiv 599 \pmod{9},$$

$$8x \equiv 5 \pmod{9}^1),$$

$$3 + \text{Ind. } x \equiv 5 \pmod{6},$$

$$\text{Ind. } x \equiv 2 \pmod{6},$$

$$x \equiv 4 \pmod{9},$$

$$x = 4 + 9k.$$

Wird dieser Wert in die vorgelegte Kongruenz eingesetzt, so ergibt sich

$$53(4 + 9k) \equiv 599 \pmod{882},$$

$$212 + 9 \cdot 53k \equiv 599 \pmod{882},$$

$$9 \cdot 53k \equiv 387 \pmod{882},$$

$$53k \equiv 43 \pmod{98},$$

$$10 + \text{Ind. } k \equiv 6 \pmod{42},$$

$$\text{Ind. } k \equiv -4 \equiv 38 \pmod{42},$$

$$k \equiv 23 \pmod{98},$$

$$k = 23 + 98k'.$$

¹⁾ Wenn wir nicht die Indizes hätten anwenden wollen, so würden wir, da $8 \equiv -1 \pmod{9}$ ist, $-x \equiv 5$, $x \equiv -5 \equiv 4 \pmod{9}$ geschlossen haben.

Es ist also

$$x = 4 + 9(23 + 98k') = 211 + 882k'$$

oder

$$x \equiv 211 \pmod{882}.$$

III. Aus

$$5x^3 \equiv 19 \pmod{98}$$

folgt

$$\text{Ind. } 5 + 3 \cdot \text{Ind. } x \equiv \text{Ind. } 19 \pmod{42},$$

$$29 + 3 \cdot \text{Ind. } x \equiv 35 \pmod{42},$$

$$3 \cdot \text{Ind. } x \equiv 6 \pmod{42},$$

$$\text{Ind. } x \equiv 2 \pmod{14}.$$

Ind. x hat also die drei Werte 2, 16, 30, und diesen entsprechen auch drei Werte von x , nämlich 9, 25, 15.

§. 95.

Der Modul 2^x . — Verteilung der Zahlen, die prim zu 2^x und kleiner als 2^x sind, unter die Divisoren von 2^{x-1} .

Der Fall, in welchem der Modul eine Potenz von 2 ist, erfordert eine besondere Behandlung. Prim zu demselben sind die ungeraden Zahlen. Wir haben also zu untersuchen, wie sich die Zahlen

$$(1) \quad 1, 3, 5, \dots, 2^x - 1$$

unter die Divisoren von $\varphi(2^x) = 2^{x-1}$ als Exponenten verteilen.

Wenn $x = 1$ ist, so kommt nur die Zahl 1 in Betracht, und diese gehört zum Exponenten 1.

Wenn $x = 2$, der Modul also 4 ist, so handelt es sich um die Zahlen 1 und 3, von denen die erste zum Exponenten 1, die zweite zum Exponenten 2 gehört. In diesen beiden Fällen kann man auch von primitiven Wurzeln sprechen, indem man als primitive Wurzel von 2 und 4 beziehungsweise die Zahlen 1 und 3 annimmt.

Wenn $x > 2$ ist, so giebt es, wie wir in §. 90 gesehen haben, keine zum Exponenten $\varphi(2^x) = 2^{x-1}$ gehörende Zahl, d. i. keine primitive Wurzel, da für jede ungerade Zahl a schon

$$a^{2^{x-2}} \equiv 1 \pmod{2^x}$$

ist. Die Zahlen der Reihe (1) verteilen sich also unter die Exponenten

$$1, 2, 2^2, \dots, 2^{x-2},$$

und es ist leicht, diese Verteilung vorzunehmen.

Die Zahl 1 gehört, wie schon bemerkt, zum Exponenten 1. Jede andere ungerade Zahl kann auf die Form

$$a = 2^n k \pm 1$$

gebracht werden, wo k ungerade und $n \geq 2$ ist. Daraus ergibt sich

$$a^2 = 2^{2n} k^2 \pm 2^{n+1} k + 1 = 2^{n+1} k(2^{n-1} k \pm 1) + 1$$

oder, wenn wir die augenscheinlich ungerade Zahl

$$k(2^{n-1} k \pm 1) = k_1$$

setzen,

$$a^2 = 2^{n+1} k_1 + 1.$$

Soll nun a^2 zum Exponenten 2 gehören, also $a^2 \equiv 1 \pmod{2^x}$ sein, so muß 2^{n+1} ein Vielfaches von 2^x , also

$$n + 1 \geq x$$

sein.

Die Annahme $n + 1 = x$ ergibt

$$n = x - 1, \quad a = 2^{x-1} k \pm 1,$$

und damit a kleiner als der Modul 2^x sei, ist $k = 1$ anzunehmen. Zum Exponenten 2 für den Modul 2^x gehören also zunächst die beiden Zahlen $2^{x-1} \pm 1$.

Wird weiter

$$n + 1 > x, \text{ also } n > x - 1$$

angenommen, so muß, da $a = 2^n k \pm 1$ kleiner als 2^x sein soll, $n = x$ und $k = 1$ angenommen und das Zeichen $\pm$ durch $-$ ersetzt werden. So erhalten wir als dritte zum Exponenten 2 gehörende Zahl $2^x - 1$. Zum Exponenten 2 gehören für den Modul 2^x , $x > 2$, also die drei Zahlen

$$2^{x-1} - 1, \quad 2^{x-1} + 1, \quad 2^x - 1.$$

Um allgemein die Zahlen zu bestimmen, die zum Exponenten 2^m , $m > 1$ gehören, betrachten wir die Gleichungen

$$\begin{aligned} a &= 2^n k \pm 1, \\ a^2 &= 2^{n+1} k_1 + 1, \\ a^{2^2} &= 2^{n+2} k_2 + 1, \\ &\dots \dots \dots, \\ a^{2^m} &= 2^{n+m} k_m + 1, \end{aligned}$$

in denen $k, k_1, k_2, \dots, k_m$ ungerade Zahlen bezeichnen. Die Zahl a wird für den Modul 2^x zum Exponenten 2^m gehören, wenn 2^{x-m} ein Vielfaches von 2^x , also

$$n + m \geq x, \quad n \geq x - m$$

ist.

Wäre $n > x - m$, etwa $n = x - m + \mu$, wo μ eine ganze positive Zahl bedeutet, so würde

$$a = 2^{x-m+\mu} k \pm 1$$

sein, und daraus würde

$$a^{2^{m-\mu}} = 2^x k_{m-\mu} + 1$$

folgen; es wäre also

$$a^{2^{m-\mu}} \equiv 1 \pmod{2^x},$$

d. h. a würde nicht zu 2^m , sondern zu dem kleineren Exponenten $2^{m-\mu}$ gehören. Die Annahme $n > x - m$ ist daher unzulässig, und wir haben $n = x - m$, also

$$a = 2^{x-m} k \pm 1$$

anzunehmen. Es ergibt sich somit das Resultat:

Um für den Modul 2^x , $x > 2$ alle zum Exponenten 2^m , $m > 1$ gehörenden Zahlen zu erhalten, haben wir in dem Ausdruck

$$a = 2^{x-m} k \pm 1$$

k alle ungeraden Werte zu erteilen, für welche $a < 2^x$ ist. Es sind dies die 2^{m-1} Werte

$$1, 3, 5, \dots, 2^m - 1.$$

Zum Exponenten 2^m gehören also — wegen des Zeichens $\pm$ im Ausdruck für a — zweimal 2^{m-1} , d. i. 2^m Zahlen, nämlich

$$2^{x-m} \cdot 1 \pm 1, 2^{x-m} \cdot 3 \pm 1, \dots, 2^{x-m} (2^m - 1) \pm 1.$$

Beispiel. Für den Modul $2^6 = 64$ ergibt sich die Tabelle:

Exponent	Zugehörige Zahlen								Summe
1	1								1
2	31	33	63						127 $\equiv$ - 1
4	15	17	47	49					128 $\equiv$ 0
8	7	9	23	25	39	41	55	57	256 $\equiv$ 0
16	3	5	11	13	19	21	27	29	512 $\equiv$ 0
	35	37	43	45	51	53	59	61	

Lehrsatz. Wenn die Zahlen $2a \pm 1$ für den Modul 2^κ ($\kappa > 2$) zum Exponenten 2^m gehören, so gehören $4a \pm 1$ zum Exponenten 2^{m-1} , $8a \pm 1$ zum Exponenten 2^{m-2} , u. s. w.

Beweis. Unter der gemachten Voraussetzung ist, wie wir oben gesehen haben,

$$2a \pm 1 = 2^{\kappa-m} k \pm 1,$$

wo k eine ungerade Zahl bezeichnet. Daraus folgt

$$4a \pm 1 = 2^{\kappa-(m-1)} k \pm 1,$$

$$8a \pm 1 = 2^{\kappa-(m-2)} k \pm 1,$$

$$\dots \dots \dots$$

folglich gehören die Zahlen $4a \pm 1$ zum Exponenten 2^{m-1} , u. s. w.

Mit Hilfe dieses Satzes kann man die Verteilung der ungeraden Zahlen unter die Divisoren von 2^κ auch in der Weise ausführen, daß man mit dem höchsten Exponenten, d. i. $2^{\kappa-1}$, beginnt und dann rückwärts zu den vorhergehenden Exponenten übergeht. Es bleiben bei diesem Verfahren zuletzt noch die Zahlen 1 und $2^\kappa - 1$ zurück, von denen die erste zum Exponenten 1, die zweite zum Exponenten 2 gehört.

§. 96.

Indizes, wenn der Modul eine Potenz von 2 ist.

Wir betrachten die Zahlen, die für den Modul 2^κ zum höchsten in Betracht kommenden Exponenten, d. i. $2^{\kappa-2}$, gehören. Für den Modul $2^3 = 8$ ist das der Exponent 2, und zu diesem gehören nach §. 95 die drei Zahlen 3, 5, 7.

Wenn $\kappa > 3$ ist, so gehören nach dem in §. 95 erhaltenen Resultat, da jetzt $m = \kappa - 2$, also $\kappa - m = 2$ ist, zum Exponenten $2^m = 2^{\kappa-2}$ die $2^{\kappa-2}$ Zahlen

$$2^2 \pm 1, 2^2 \cdot 3 \pm 1, 2^2 \cdot 5 \pm 1, \dots, 2^2(2^{\kappa-2} - 1) \pm 1,$$

also alle Werte, welche der Ausdruck $4k \pm 1$ annimmt, wenn man k der Reihe nach gleich

$$1, 3, 5, \dots, 2^{\kappa-2} - 1$$

setzt. Nimmt man $k = 2k' + 1$ an, so wird

$$a = 4(2k' + 1) \pm 1,$$

also entweder

$$8k' + 5 \text{ oder } 8k' + 3,$$

und diese beiden Ausdrücke liefern alle zum Exponenten 2^{x-2} gehörenden Zahlen, wenn k' die Werte

$$0, 1, 2, 3, \dots, 2^{x-3} - 1$$

beigelegt werden. Man erhält dadurch $2 \cdot 2^{x-3} = 2^{x-2}$ inkongruente Zahlen, die sämtlich kleiner als der Modul sind und zum Exponenten 2^{x-2} gehören, also alle zu diesem Exponenten gehörenden Zahlen.

Nun beträgt die Anzahl der unterhalb 2^x liegenden ungeraden Zahlen 2^{x-1} . Da von jeder der vier Formen

$$8k + 1, 8k + 3, 8k + 5, 8k + 7$$

gleich viel vorhanden sind, so kommen auf die beiden Formen

$$8k + 3, \quad 8k + 5$$

die Hälfte, d. i. 2^{x-2} dieser Zahlen. Es gehören somit alle Zahlen $8k + 3, 8k + 5$ und nur diese zum höchsten in Betracht kommenden Exponenten, d. i. zu 2^{x-2} .

Wir nehmen jetzt eine beliebige Zahl a einer dieser beiden Formen

$$8k + 3, \quad 8k + 5,$$

etwa der ersteren Form, und betrachten ihre Potenzen

$$a, a^2, a^3, \dots, a^{2^{x-2}}.$$

Wir erhalten

$$\begin{array}{ll} a = 8k_1 + 3, & a^2 = 8k_2 + 1, \\ a^3 = 8k_3 + 3, & a^4 = 8k_4 + 1, \\ \dots & \dots \end{array}$$

wo $k_1, k_2, k_3, \dots$ ganze Zahlen bezeichnen. Offenbar sind danach die 2^{x-2} ungeraden Potenzen sämtlich von der Form $8k + 3$, die 2^{x-2} geraden Potenzen sämtlich von der Form $8k + 1$. Da nun a zum Exponenten 2^{x-2} gehört, diese Potenzen von a also sämtlich inkongruent sind, und da es unter 2^x eben 2^{x-2} Zahlen jeder der beiden Formen $8k + 1, 8k + 3$ giebt, so erhalten wir das Resultat: Jede Zahl $8k + 1, 8k + 3$, die kleiner als der Modul ist, kann als Potenz von a dargestellt werden.

Wenn man die Zeichen der Zahlen $8k + 1, 8k + 3$ ändert, oder, was hinsichtlich der Kongruenz dasselbe ist, ihre Er-

gänzungen zum Modul nimmt, so erhält man alle Zahlen

$$8k + 7, \quad 8k + 5.$$

Ebenso kann man alle Zahlen

$$8k + 1, \quad 8k + 5$$

als Potenzen einer Zahl a der Form $8k + 5$ darstellen; die Ergänzungen dieser Zahlen zum Modul sind die Zahlen

$$8k + 7, \quad 8k + 3.$$

Somit läßt sich jede unterhalb des Moduls 2^x liegende ungerade Zahl oder ihre Ergänzung zum Modul durch eine Potenz einer Zahl der Form $8k + 3$ oder der Form $8k + 5$ ersetzen.

Ist g eine Zahl einer dieser beiden Formen, und hat sich

$$n \equiv g^i \equiv g^{i+2^{x-2}} \pmod{2^x}$$

ergeben, so nennt man wieder i den Index von n und schreibt

$$\text{Ind. } n \equiv i \pmod{2^{x-2}}.$$

In die Tafeln des Anhangs sind die Indizes der in Betracht kommenden Zahlen für die Moduln 8, 16, 32, 64 aufgenommen. Als primitive Wurzel ist dabei überall die Zahl 3 gewählt.

§. 97.

Anwendung der Indizes zur Auflösung der linearen und der binomischen Kongruenz für den Modul 2^x .

Auch die Indizes, zu denen uns der Modul 2^x geführt hat, lassen sich ohne weiteres zur Auflösung der Kongruenz ersten Grades und der binomischen Kongruenz für diesen Modul benutzen. Nur hat man nicht zu vergessen, so oft in der Kongruenz eine Zahl $8k + 5$ oder $8k + 7$ auftritt, statt derselben ihre mit entgegengesetztem Zeichen versehene Ergänzung zum Modul zu nehmen.

Beispiele. I.

$$\begin{aligned} 13x &\equiv 27 \pmod{32}, \\ 19(-x) &\equiv 27 \pmod{32}, \\ \text{Ind. } 19 + \text{Ind. } (-x) &\equiv \text{Ind. } 27 \pmod{8}, \\ 5 + \text{Ind. } (-x) &\equiv 3 \pmod{8}, \\ \text{Ind. } (-x) &\equiv -2 \equiv 6 \pmod{8}, \\ -x &\equiv 25 \pmod{32}, \\ x &\equiv -25 \equiv 7 \pmod{32}. \end{aligned}$$

II.

$$\begin{aligned}
 15x &\equiv 29 \pmod{64}, \\
 -49x &\equiv -35 \pmod{64}, \\
 49x &\equiv 35 \pmod{64}, \\
 12 + \text{Ind. } x &\equiv 9 \pmod{16}, \\
 \text{Ind. } x &\equiv -3 \equiv 13 \pmod{16}, \\
 x &\equiv 19 \pmod{64}.
 \end{aligned}$$

III.

$$\begin{aligned}
 3x^5 &\equiv 31 \pmod{64}, \\
 3(-x)^5 &\equiv 33 \pmod{64}, \\
 \text{Ind. } 3 + 5 \cdot \text{Ind. } (-x) &\equiv \text{Ind. } 33 \pmod{16}, \\
 1 + 5 \cdot \text{Ind. } (-x) &\equiv 8 \pmod{16}, \\
 5 \cdot \text{Ind. } (-x) &\equiv 7 \pmod{16}, \\
 11 \cdot \text{Ind. } (-x) &\equiv 9 \pmod{16}, \\
 \text{Ind. } 11 + \text{Ind. Ind. } (-x) &\equiv \text{Ind. } 9 \pmod{4}, \\
 3 + \text{Ind. Ind. } (-x) &\equiv 2 \pmod{4}, \\
 \text{Ind. Ind. } (-x) &\equiv -1 \equiv 3 \pmod{4}, \\
 \text{Ind. } (-x) &\equiv 11 \pmod{16}, \\
 -x &\equiv 59 \pmod{64}, \\
 x &\equiv -59 \equiv 5 \pmod{64}.
 \end{aligned}$$

§. 98.

Die binomische Kongruenz im Falle eines beliebig zusammengesetzten Moduls.

Es sei

$$m = 2^\kappa p^\lambda q^\mu \dots,$$

wo $p, q, \dots$ ungerade Primzahlen, $\kappa, \lambda, \mu, \dots$ ganze positive Zahlen bezeichnen. Soll nun

$$ax^\kappa \equiv b \pmod{m}^1),$$

also $ax^\kappa - b$ durch m teilbar sein, so muß, da die Zahlen

$$2^\kappa, p^\lambda, q^\mu, \dots$$

prim zu einander sind, jede derselben in $ax^\kappa - b$ aufgehen, d. h. es müssen die folgenden Kongruenzen bestehen:

¹⁾ Der verallgemeinerte Fermatsche Satz (§. 88) gestattet auch hier, den Koeffizienten von x^κ auf die Einheit zu reduzieren. Zu diesem Zwecke hat man, da $a\varphi(m) \equiv 1 \pmod{m}$ ist, beide Seiten der Kongruenz mit $a^{-1+\varphi(m)}$ zu multiplizieren.

$$\begin{aligned} ax^n &\equiv b \pmod{2^*}, \\ ax^n &\equiv b \pmod{p^2}, \\ &\dots \end{aligned}$$

Wenn eine dieser Kongruenzen unmöglich ist, so ist es auch die vorgelegte Kongruenz. Wenn dagegen x_1 eine Wurzel der ersten, x_2 eine Wurzel der zweiten Kongruenz, u. s. w. bezeichnet, so wird die vorgelegte Kongruenz durch jede Zahl X befriedigt, welche den Bedingungen

$$X \equiv x_1 \pmod{2^*}, \quad X \equiv x_2 \pmod{p^2}, \quad \dots$$

genügt. Die Aufgabe ist also auf die in §. 38 behandelte zurückgeführt.

Beispiel

$$11x^3 \equiv 14843 \pmod{39200}.$$

$$\text{Es ist } 39200 = 2^5 \cdot 5^2 \cdot 7^2.$$

- 1) $11x^3 \equiv 14843 \pmod{32},$
 $11x^3 \equiv 27 \pmod{32},$
 $7 + 3.\text{Ind. } x \equiv 3 \pmod{8},$
 $3.\text{Ind. } x \equiv -4 \equiv 4 \pmod{8},$
 $\text{Ind. } x \equiv 4 \pmod{8},$
 $x \equiv 17 \pmod{32}.$
- 2) $11x^3 \equiv 14843 \equiv 18 \pmod{25},$
 $16 + 3.\text{Ind. } x \equiv 15 \pmod{20},$
 $3.\text{Ind. } x \equiv -1 \pmod{20},$
 $\text{Ind. } x \equiv 13 \pmod{20},$
 $x \equiv 17 \pmod{25}.$
- 3) $11x^3 \equiv 14843 \pmod{49},$
 $11x^3 \equiv 45 \pmod{49},$
 $40 + 3.\text{Ind. } x \equiv 31 \pmod{42},$
 $3.\text{Ind. } x \equiv -9 \pmod{42},$
 $\text{Ind. } x \equiv -3 \equiv 11 \pmod{14},$
 $\text{Ind. } x \equiv 11, 25, 39 \pmod{42},$
 $x \equiv 12, 17, 20 \pmod{49}.$

Der §. 38 liefert dann für X die drei Werte

$$X \equiv 12017, \quad 17, \quad -7183 \pmod{39200}.$$

§. 99.

Über die Divisoren der Zahl $a^m - 1$.

Die Aufgabe, eine Zahl N in ihre Faktoren zu zerlegen, macht, wenn N einigermaßen groß ist, nicht geringe Mühe. Um nämlich die kleinste in N aufgehende Primzahl zu finden, muß man N der Reihe nach durch die einzelnen Primzahlen, von der kleinsten anfangend, dividieren. Hat man N durch alle unterhalb $\sqrt{N}$ liegenden Primzahlen dividiert und jedesmal einen von Null verschiedenen Rest erhalten, so weiß man, daß N selbst eine Primzahl ist. Wenn sich aber herausgestellt hat, daß eine Primzahl p in N aufgeht, so ist

$$N = p \cdot \frac{N}{p},$$

und es bleibt nur noch $\frac{N}{p}$ in Faktoren zu zerlegen. Hierfür ist es offenbar überflüssig, nochmals die Divisionen mit den Primzahlen, die kleiner als p sind, zu versuchen; denn wenn eine solche, etwa q in $\frac{N}{p}$ aufginge, so müßte sie auch in N aufgehen, und das hätte sich, da $q < p$ ist, schon bei den Divisionen herausgestellt, die behufs der Zerlegung von N versucht sind, und die zur Auffindung des Primfaktors p geführt haben. Um $\frac{N}{p}$ zu zerlegen, hat man also die Divisionen mit (nochmals) p und weiter denjenigen Primzahlen zu versuchen, die zwischen p und

$$\sqrt{\frac{N}{p}}$$

liegen. Auf diese Weise erhält man entweder einen neuen Primfaktor p' von N , oder man überzeugt sich, daß $\frac{N}{p}$ eine Primzahl ist. So fortfahrend kann man allmählich sämtliche Primfaktoren von N ermitteln.

Die Zahlenlehre setzt uns nun in vielen Fällen in den Stand, dieses primitive Verfahren abzukürzen. Indem sie uns lehrt, daß Zahlen von bestimmter Form nur Primzahlen bestimmter Formen

als Divisoren zulassen, dagegen durch Primzahlen anderer Formen auf keinen Fall teilbar sind, verringert sie die Anzahl der zu versuchenden Divisionen, und dadurch wird oft eine ganz erhebliche Vereinfachung der Sache herbeigeführt.

Eine ausführliche Behandlung des Gegenstandes würde mehr Kenntnisse in der Zahlenlehre voraussetzen, als durch dieses Buch vermittelt werden. Hier sollen nur die beiden Formen $a^m + 1$ ¹⁾ betrachtet werden, in denen m eine ganze positive Zahl bezeichnet. Hinsichtlich der Zahlen $a^m - 1$ gelten folgende Sätze:

Lehrsatz I. Es sei p eine ungerade Primzahl und d der größte gemeinschaftliche Divisor von $m = \mu d$ und $p - 1 = kd$, so daß μ prim zu k und $p = kd + 1$ ist. Wenn dann $a^m - 1$ durch p teilbar ist, so muß p auch in $a^d - 1$ aufgehen.

Beweis. Da a eine Wurzel der Kongruenz $x^m \equiv 1 \pmod{p}$ und d der größte gemeinschaftliche Divisor von m und $p - 1$ ist, so muß nach dem Zusatz des §. 79 a auch die Kongruenz $x^d \equiv 1 \pmod{p}$ befriedigen, d. h. p muß in $a^d - 1$ aufgehen.

Beispiel. Da $5^8 - 1 = 390624$ durch 13 teilbar und 4 der größte gemeinschaftliche Divisor von 8 und $13 - 1 = 12$ ist, so geht 13 auch in $5^4 - 1$ auf.

Lehrsatz II. Es sei $2n + 1$ eine Primzahl. Dann müssen diejenigen ungeraden Primzahlen, welche Divisoren von $a^{2n+1} - 1$ sind, entweder die Form

$$2(2n + 1)k + 1$$

haben oder in $a - 1$ aufgehen.

Beweis. Es sei $p = 2l + 1$ eine ungerade Primzahl. Wenn dann l durch $2n + 1$ teilbar, etwa

$$\frac{l}{2n + 1} = k$$

ist, so ergibt sich

$$p = 2(2n + 1)k + 1.$$

¹⁾ Es würde nicht allgemeiner sein, die Formen $a^m \pm b^m$ zu betrachten, wo a und b teilerfremde Zahlen sind. Denn wenn eine dieser Formen durch die Primzahl p teilbar ist, so kann man immer $a = bx + py$ machen, und dann wird auch $x^m \pm 1$ durch p teilbar sein müssen. (Legendre, Théorie des Nombres I, p. 222.)

Wenn dagegen l durch die Primzahl $2n + 1$ nicht teilbar ist, so ist l und ebenso $2l$ prim zu $2n + 1$, der größte gemeinschaftliche Divisor beider Zahlen also gleich 1.

Nehmen wir jetzt an, $p = 2l + 1$ sei ein Divisor von $a^{2n+1} - 1$, und es sei zugleich $p - 1 = 2l$ prim zu $2n + 1$. Dann muß nach Lehrsatz I p ein Divisor von $a^1 - 1$, d. i. von $a - 1$ sein. Wenn dagegen l , also auch $2l$, durch $2n + 1$ teilbar ist, so hat, wie wir gesehen haben, p die Form

$$2(2n + 1)k + 1,$$

und da nur diese beiden Fälle möglich sind, so ist der Satz bewiesen.

Zusatz. Wenn $2n + 1$ eine Primzahl ist, so hat jede in $2^{2n+1} - 1$ aufgehende Primzahl die Form

$$2(2n + 1)k + 1.$$

Beispiele. I. Eine in $10^7 - 1$ aufgehende ungerade Primzahl muß entweder die Form $14k + 1$ haben oder ein Divisor von $10 - 1 = 9$ sein. Es ergibt sich zunächst

$$10^7 - 1 = 9.1111111,$$

und um 1111111 zu zerlegen, hat man die Division mit den unter $\sqrt{1111111}$ liegenden Primzahlen der Form $14k + 1$ zu versuchen. Man erhält

$$10^7 - 1 = 9.239.4649.$$

II. Eine in $2^{11} - 1 = 2047$ aufgehende Primzahl muß $< \sqrt{2047}$ und von der Form $22k + 1$ sein. Man erhält

$$2^{11} - 1 = 23.89.$$

III. Es soll $5^7 - 1 = 78124$ in Faktoren zerlegt werden. Man findet zunächst $5^7 - 1 = 4.19531$, und um den letzten Faktor zu untersuchen, hat man der Reihe nach mit den Primzahlen der Form $14k + 1$, die $< \sqrt{19531} \sim 139$ sind, zu dividieren. Es sind dies die fünf Zahlen 29, 43, 71, 113, 127. Da keine derselben aufgeht, so ist 19531 eine Primzahl und die Zerlegung beendet.

IV. Ein Divisor von $2^{31} - 1 = 2147483647$ müßte von der Form $62k + 1$ sein und zugleich, da er auch in $2^{32} - 2$ aufgehen, also zu den Primzahlen gehören müßte, für welche 2 ein quadratischer Rest wäre, einer der beiden Formen $8n + 1$,

$8n + 7$ angehören (s. §. 116). Es ergeben sich daraus für diesen Divisor die beiden Formen

$$248k + 1, \quad 248k + 63.$$

Eine obere Grenze für ihn ist zugleich

$$\sqrt{2^{31} - 1} \sim 46340.$$

Euler hat alle erforderlichen Divisionen versucht und gefunden, daß $2^{31} - 1$ eine Primzahl ist (Commentationes arithmet. collectae I, p. 584).

V. $2^{37} - 1 = 137438953471$ ist, wie Fermat (Varia Opera math. p. 177 = Oeuvres II, p. 199) gefunden hat, durch 223 teilbar.

§. 100.

Divisoren der Zahl $a^m + 1$.

Lehrsatz I. Wenn die ungerade Primzahl p ein Divisor von $a^m + 1$ ist, so hat sie die Form

$$p = 2kd + 1,$$

wo d der größte gemeinschaftliche Divisor von m und $p - 1$, $\frac{m}{d}$ ungerade und prim zu $\frac{p-1}{2d}$ ist. Außerdem ist p auch ein Divisor von $a^d + 1$.

Beweis. Die Kongruenz

$$x^m \equiv -1 \equiv p - 1 \pmod{p}$$

liefert, wenn beiderseits die Indizes für irgend eine Basis genommen werden, da nach einem in §. 86 mitgetheilten Satze der

Index von $p - 1$ für jede Basis $= \frac{1}{2} (p - 1)$ ist,

$$m \text{ Ind. } x \equiv \frac{1}{2} (p - 1) \pmod{p - 1}.$$

Es sei nun d der größte gemeinschaftliche Divisor von m und $p - 1$, etwa

$$m = \mu d, \quad p - 1 = p' d.$$

Dann sind μ und p' prim zu einander, und man erhält durch Division der letzten Kongruenz mit d

$$\mu \text{ Ind. } x \equiv \frac{1}{2} p' \pmod{p'}.$$

Damit diese, also auch die vorgelegte Kongruenz, möglich sei, muß

$$p' = \frac{p-1}{d}$$

eine gerade Zahl sein, und wenn diese Bedingung erfüllt ist, hat die vorgelegte Kongruenz d Wurzeln.

Unter der gemachten Voraussetzung hat aber auch, wie ebenfalls durch Übergang zu den Indizes bewiesen wird, die Kongruenz

$$x^d \equiv -1 \equiv p-1 \pmod{p}$$

d Wurzeln, und es läßt sich leicht zeigen, daß jede der letzteren auch die Kongruenz $x^m \equiv -1 \pmod{p}$ befriedigt.

Da nämlich μ und p' prim zu einander sind und p' eine gerade Zahl ist, so muß μ ungerade, also $(-1)^\mu = -1$ sein. Bezeichnet nun a eine beliebige Wurzel der Kongruenz

$$x^d \equiv -1 \pmod{p},$$

so ist $a^d \equiv -1$, folglich $a^{\mu d}$, d. i.

$$a^m \equiv (-1)^\mu \equiv -1 \pmod{p},$$

d. h. a ist auch eine Wurzel der Kongruenz $x^m \equiv -1 \pmod{p}$. Die beiden Kongruenzen

$$x^m \equiv -1, \quad x^d \equiv -1 \pmod{p}$$

stimmen somit hinsichtlich der Wurzeln vollständig überein.

Wenn wir p' , d. i. $\frac{p-1}{d} = 2k$ setzen, so erhalten wir

$p = 2kd + 1$, und da wir oben gesehen haben, daß $\frac{m}{d} = \mu$

ungerade und prim zu der geraden Zahl $p' = \frac{p-1}{d}$, also auch

prim zu $\frac{p-1}{2d}$ ist, so ist der Satz bewiesen.

Lehrsatz II. Eine ungerade Primzahl p , welche ein Divisor von $a^{2n+1} + 1$ ist, hat entweder die Form

$$p = 2(2n+1)k + 1,$$

oder sie ist ein Divisor von $a + 1$.

Beweis. Es sei $p = 2v + 1$. Wenn dann v durch $2n+1$ teilbar, etwa $v = (2n+1)k$ ist, so erhält man $p = 2(2n+1)k + 1$.

Wenn dagegen ν , also auch $2\nu = p - 1$ prim zu $2^n + 1$ ist, so ist der grösste gemeinschaftliche Divisor von $p - 1$ und $2^n + 1$ gleich 1, und dann muſs p nach dem Lehrsatz I ein Divisor von $a + 1$ sein.

Zusatz. Ein jeder Divisor von $2^{2^n} + 1$ ist von der Form $2^{n+1}k + 1$.

Beweis. Nach dem Lehrsatz I ist ein Divisor der vorgelegten Zahl von der Form $p = 2kd + 1$. Dabei muſs

$$\frac{m}{d} = \frac{2^n}{d}$$

ungerade sein. Das ist nur für $d = 2^n$ der Fall, und somit ist

$$p = 2 \cdot 2^n k + 1 = 2^{n+1}k + 1.$$

Beispiele. I. Die Divisoren von

$$2^{2^5} + 1 = 2^{32} + 1 = 4294967297$$

müssen von der Form $64k + 1$ sein. Die Primzahlen dieser Form sind

$$193, 257, 449, 577, 641, 769, 1153, \dots$$

Man findet

$$2^{32} + 1 = 641 \cdot 6700417.$$

Durch dieses Beispiel hat Euler (Commentationes arithmet. collectae I, 356) die Vermutung Fermats, daſs $2^{2^n} + 1$ für jeden Wert von n eine Primzahl liefere, widerlegt (s. §. 8, S. 14). 6700417 ist, wie Euler gefunden hat, eine Primzahl.

II. Es soll $10^{11} + 1$ in Faktoren zerlegt werden. Eine in diese Zahl aufgehende ungerade Primzahl muſs entweder in $10 + 1 = 11$ aufgehen oder die Form $22k + 1$ haben. Man erhält zunächst

$$10^{11} + 1 = 11 \cdot 11 \cdot 926446281.$$

Die kleinste Primzahl der Form $22k + 1$ ist 23. Diese geht in den noch zu zerlegenden Faktor auf, und es ergibt sich schlieſslich

$$10^{11} + 1 = 11 \cdot 11 \cdot 23 \cdot 35932447 = 11^2 \cdot 23 \cdot 4093 \cdot 8779.$$

Die Zerlegung ist Johann Bernoulli, der das Beispiel in einer Arbeit über die Divisoren der Summe

$$S = 1 + 10^1 + 10^2 + \dots + 10^n$$

vorgenommen hat (Nouveaux Mémoires de l'Académie royale des Sciences et Belles-Lettres. Berlin 1771, S. 325), wohl infolge

eines schon bei der Division mit 11 gemachten Rechenfehlers nicht gelungen. Erst Seelhoff hat die Aufgabe zu Ende geführt.

III. Es ist

$$2^{32} - 1 = (2 - 1)(2 + 1)(2^2 + 1)(2^4 + 1)(2^8 + 1)(2^{16} + 1) \\ = 1.3.5.17.257.65537,$$

und da 65537 nach §. 88 eine Primzahl ist, so ist die Zerlegung beendet.

§. 101.

Verwandlung gemeiner Brüche in Dezimalbrüche
(Gauss, Werke Bd. I, S. 382 und Bd. II, S. 412).

„Wenn ein Bruch in einen Dezimalbruch verwandelt wird, so nennen wir die Reihe der Dezimalstellen, mag dieselbe nun endlich sein oder unbegrenzt fortgehen, die Mantissee des Bruches, indem wir diesen sonst nur bei den Logarithmen gebrauchten Ausdruck in weiterem Sinne nehmen. (Die etwa vorhandenen ganzen Zahlen werden dabei ausgeschlossen.) So ist 125 die Mantissee von $\frac{1}{8}$, 1875 die Mantissee des Bruches $\frac{35}{16}$, 054054 ... in inf. die Mantissee von $\frac{2}{37}$.

Aus dieser Definition geht hervor, daß zwei Brüche $\frac{l}{n}$, $\frac{m}{n}$ mit demselben Nenner n dieselben oder verschiedene Mantissen haben, je nachdem die Zähler l , m für den Modul n kongruent sind oder nicht. Eine endliche Mantissee ändert sich nicht, wenn rechts beliebig viele Nullen angehängt werden. Man erhält die Mantissee des Bruches $\frac{10^v m}{n}$, indem man die erste Ziffer der Man-

tisse von $\frac{m}{n}$ abschneidet. Allgemein bildet man die Mantissee des

Bruches $\frac{10^v m}{n}$, indem man die v ersten Ziffern der Mantissee von

$\frac{m}{n}$ abschneidet. Die Mantissee von $\frac{1}{n}$ fängt gleich mit einer von Null verschiedenen Ziffer an, wenn n nicht größer als 10 ist. Wenn dagegen $n > 10$, keine Potenz von 10 und eine k stellige Zahl ist, so werden die $k - 1$ ersten Ziffern der Mantissee Null, und erst die k te Ziffer wird von Null verschieden sein. Daraus folgt

leicht, daß, wenn $\frac{l}{n}, \frac{m}{n}$ verschiedene Mantissen haben (d. i. wenn l und m für den Modul n inkongruent sind), diese Mantissen sicherlich in den k ersten Stellen nicht übereinstimmen können, sondern wenigstens in der k^{ten} Stelle verschieden sein müssen.“

„Wir fangen mit der Betrachtung von Brüchen an, deren Nenner Primzahlen oder Potenzen von Primzahlen sind; darauf werden wir zeigen, wie die übrigen Brüche auf Brüche der genannten Art zurückgeführt werden. Zunächst bemerken wir, daß die Mantisse des Bruches $\frac{a}{p^\mu}$ (dessen Zähler a wir immer als durch die Primzahl p nicht teilbar voraussetzen) endlich ist und aus μ Ziffern besteht, wenn $p = 2$ oder $= 5$ ist. Im ersteren Falle wird diese Mantisse, als ganze Zahl angesehen, $5^\mu a$ sein, im zweiten $2^\mu a$. Das ist so einleuchtend, daß es keiner weiteren Erklärung bedarf.

„Wenn dagegen p eine andere Primzahl ist, so wird $10^e a$ niemals durch p^μ teilbar sein, wie groß man auch e annehmen möge, und daraus folgt, daß die Mantisse des Bruches

$$F = \frac{a}{p^\mu}$$

notwendiger Weise unbegrenzt fortgeht. Nehmen wir an, 10^e sei die niedrigste Potenz von 10, die für den Modul p^μ der Einheit kongruent ist (e ist dann, wie wir gezeigt haben, entweder gleich $(p - 1)p^{\mu-1}$ oder ein Divisor dieser Zahl), so erkennen wir leicht, daß $10^e a$ die erste Zahl in der Reihe

$$10 a, 100 a, 1000 a, \dots$$

sein wird, welche für denselben Modul der Zahl a selbst kongruent ist. Da nun, wie wir oben gesehen haben, die Mantissen der Brüche

$$\frac{10 a}{p^\mu}, \frac{100 a}{p^\mu}, \dots, \frac{10^e a}{p^\mu}$$

dadurch erhalten werden, daß man von der Mantisse des Bruches F beziehungsweise die erste, die beiden ersten, ..., die e ersten Stellen abschneidet, so leuchtet ein, daß in dieser Mantisse nach den ersten e Stellen, aber nicht früher, dieselben Ziffern wiederkehren. Die ersten e Ziffern, die, unendlich oft wiederholt, die

Mantisse des Bruches bilden, können wir die Periode dieser Mantisse oder des Bruches F nennen, und es ist klar, daß die Länge der Periode, das ist die Anzahl der Ziffern, aus denen sie besteht, und die gleich e ist, von dem Zähler a des Bruches ganz unabhängig ist und einzig und allein durch den Nenner bestimmt wird. So ist z. B. die Periode des Bruches $\frac{1}{11}$ gleich 09, die Periode von $\frac{3}{7}$ ist 428571.

„Sobald man also die Periode eines Bruches hat, kann man seine Mantisse beliebig weit fortsetzen. Weiter leuchtet ein, daß, wenn

$$b \equiv 10^\lambda a \pmod{p^\mu}$$

ist, man die Periode des Bruches $\frac{b}{p^\mu}$ dadurch erhält, daß man die λ ersten Ziffern der Periode von F hinter die $e - \lambda$ anderen schreibt, daß man also zugleich mit der Periode des Bruches F die Perioden aller Brüche erhält, deren Zähler den Zahlen

$$10a, 100a, 1000a, \dots$$

für den Modul p^μ kongruent sind. Da z. B.

$$6 \equiv 3 \cdot 10^3 \pmod{7}$$

ist, so ergibt sich aus der Periode von $\frac{3}{7}$ sofort 857142 als Periode von $\frac{6}{7}$.

„So oft also 10 eine primitive Wurzel des Moduls p^μ ist, kann aus der Periode von $\frac{1}{p^\mu}$ die Periode jedes anderen Bruches $\frac{m}{p^\mu}$ (dessen Zähler m durch p nicht teilbar ist) hergeleitet werden.

Man hat zu diesem Zwecke in der Periode von $\frac{1}{p^\mu}$ nur links so viele Stellen abzuschneiden und rechts anzusetzen, als der Index von m für die Basis 10 Einheiten enthält.

„Wenn dagegen 10 keine primitive Wurzel ist, so werden durch die Periode von $\frac{1}{p^\mu}$ nur die Perioden derjenigen Brüche mitbestimmt, deren Zähler Potenzen von 10 für den Modul p^μ

kongruent sind.“ Es sind das, wenn 10 zum Exponenten e gehört, $e - 1$ Brüche, wobei $\frac{1}{p^u}$ nicht mitgezählt ist. Wenn wir jetzt (durch Division) einen Bruch $\frac{a'}{p^u}$, dessen Periode noch nicht erhalten ist, in einen Dezimalbruch verwandeln, so bestimmt dessen Periode die Perioden der $e - 1$ Brüche, deren Zähler beziehungsweise den Zahlen $10a'$, $100a'$, ... für den Modul p^u kongruent sind. Auf diese Weise haben wir schon die Perioden von $2e$ Brüchen gefunden. So können wir fortfahren, bis alle irreduzibelen Brüche mit dem Nenner p^u erschöpft sind. Dieselben sind dann in

$$\frac{(p - 1) p^{u-1}}{e}$$

Reihen von je e Brüchen zerfallen.

Beispiel. Für den Modul 41 gehört 10 zum Exponenten 5. und da $\frac{40}{5} = 8$ ist, so verteilen sich die 40 Brüche mit dem Nenner 41 in acht Reihen. Nun ist mod. 41

$10^1 \equiv 10$, $10^2 \equiv 18$, $10^3 \equiv 16$, $10^4 \equiv 37$, $10^5 \equiv 1$;
folglich enthält die erste Reihe die Brüche

$$(1) \quad \frac{1}{41}, \frac{10}{41}, \frac{16}{41}, \frac{18}{41}, \frac{37}{41},$$

und da

$$\frac{1}{41} = 0,02439024 \dots$$

ist, so sind die Perioden dieser Brüche

$$02439, 24390, 39024, 43902, 90243.$$

In der Reihe (1) kommt der Bruch

$$\frac{2}{41} = 0,0487804 \dots$$

nicht vor, und da mod. 41

$2 \cdot 10 \equiv 20$, $2 \cdot 10^2 \equiv 36$, $2 \cdot 10^3 \equiv 32$, $2 \cdot 10^4 \equiv 33$, $2 \cdot 10^5 \equiv 2$
ist, so enthält die zweite Reihe die Brüche

$$(2) \quad \frac{2}{41}, \frac{20}{41}, \frac{32}{41}, \frac{33}{41}, \frac{36}{41}$$

mit den Perioden

04878, 48780, 78048, 80487, 87804.

So fortfahrend erhalten wir weiter

$$(3) \quad \frac{3}{41}, \frac{7}{41}, \frac{13}{41}, \frac{29}{41}, \frac{30}{41};$$

Perioden: 07317, 17073, 31707, 70731, 73170.

$$(4) \quad \frac{4}{41}, \frac{23}{41}, \frac{25}{41}, \frac{31}{41}, \frac{40}{41};$$

Perioden: 09756, 56097, 60975, 75609, 97560.

$$(5) \quad \frac{5}{41}, \frac{8}{41}, \frac{9}{41}, \frac{21}{41}, \frac{39}{41};$$

Perioden: 12195, 19512, 21951, 51219, 95121.

$$(6) \quad \frac{6}{41}, \frac{14}{41}, \frac{17}{41}, \frac{19}{41}, \frac{26}{41};$$

Perioden: 14634, 34146, 41463, 46341, 63414.

$$(7) \quad \frac{11}{41}, \frac{12}{41}, \frac{28}{41}, \frac{34}{41}, \frac{38}{41};$$

Perioden: 26829, 29268, 68292, 82926, 92682.

$$(8) \quad \frac{15}{41}, \frac{22}{41}, \frac{24}{41}, \frac{27}{41}, \frac{35}{41};$$

Perioden: 36585, 53658, 58536, 65853, 85365.

Was nun einen Bruch betrifft, dessen Nenner ein Produkt von Primzahlen oder Primzahlpotenzen ist, so können wir denselben nach §. 39 in Partialbrüche zerlegen, jeden der letzteren in einen Dezimalbruch verwandeln und die erhaltenen Resultate addieren. Bei diesem Verfahren kann zwar die letzte Ziffer ungenau werden, der Fehler offenbar aber nicht so viele Einheiten betragen, als Brüche addiert werden. „Es empfiehlt sich daher, für die einzelnen Brüche einige Stellen mehr hinzuschreiben, als im Resultat verlangt werden. Als Beispiel wollen wir den Bruch

$$F = \frac{6099380351}{1271808720}$$

betrachten, dessen Nenner das Produkt der Zahlen 16, 9, 5, 49, 13, 47, 59 ist. Man erhält

$$F = 1 + \frac{11}{16} + \frac{4}{9} + \frac{4}{5} + \frac{22}{49} + \frac{5}{13} + \frac{7}{47} + \frac{52}{59},$$

und die Verwandlung der einzelnen Brüche in Dezimalbrüche ergibt:

$$\begin{array}{rcl}
 1 & = & 1 \\
 \frac{11}{16} & = & 0,6875 \\
 \frac{4}{9} & = & 0,444\,444\,444\,4\quad 444\,444\,444\,4\quad 44 \\
 \frac{4}{5} & = & 0,8 \\
 \frac{22}{49} & = & 0,448\,979\,591\,8\quad 367\,346\,938\,7\quad 75 \\
 \frac{5}{13} & = & 0,384\,615\,384\,6\quad 153\,846\,153\,8\quad 46 \\
 \frac{5}{47} & = & 0,148\,936\,170\,2\quad 127\,659\,574\,4\quad 68 \\
 \frac{52}{59} & = & 0,881\,355\,932\,2\quad 033\,898\,305\,0\quad 84 \\
 \hline
 F' & = & 4,795\,831\,523\,3\quad 127\,195\,416\,6\quad 17.
 \end{array}$$

Der Fehler in dieser Summe ist jedenfalls kleiner als fünf Einheiten in der 22. Dezimalstelle, hat also auf die 20 ersten Stellen keinen Einfluss. Durch Fortsetzung der Rechnung auf mehr Stellen ergibt sich statt der 17 in den beiden letzten Stellen

1893936 . . .

Übrigens sieht jeder, auch ohne daß wir darauf aufmerksam machen, daß diese Methode der Verwandlung gemeiner Brüche in Dezimalbrüche sich namentlich in den Fällen empfiehlt, in welchen viele Stellen verlangt werden. Wenn nämlich wenig Stellen genügen, kann man sich meist ebenso bequem der gewöhnlichen Division oder der Logarithmen bedienen."

Anmerkungen. I. Gaus hat (Werke II, S. 411 bis 434) die Perioden für alle dem ersten Tausend angehörenden Primzahlen und Primzahlpotenzen gegeben. Der Hauptnutzen dieser Arbeit besteht natürlich in der Erleichterung der Verwandlung gemeiner Brüche in Dezimalbrüche. Sie leistet aber zuweilen auch Dienste, wenn Zahlen der Form $10^n - 1$ in Faktoren zerlegt werden sollen. $10^n - 1$ ist nämlich durch die Primzahl p teilbar, wenn die Periode von $\frac{1}{p}$ aus n Ziffern besteht. So z. B.

ist $10^3 - 1$ sowohl durch 73 als auch durch 137 teilbar, denn jeder der Brüche $\frac{1}{73}, \frac{1}{137}$ hat der Tabelle zufolge eine achtziffrige Periode. Man erhält auf diese Weise

$$10^3 - 1 = 3^2 \cdot 11 \cdot 73 \cdot 101 \cdot 137.$$

II. Die Periodenlänge für alle Primzahlen unterhalb 100 000 hat Friedrich Kessler¹⁾ berechnet. Seine Tabelle ist auch abgedruckt in der Programmarbeit von Heinrich Bork: „Periodische Dezimalbrüche“ (Berlin, 1895. Jahresbericht des Königl. Prinz Heinrichs-Gymnasiums).

III. Statt einen Bruch $\frac{P}{Q}$ in einen Dezimalbruch zu verwandeln, kann man ihn allgemein auf die Form

$$\alpha_0 + \frac{\alpha_1}{g} + \frac{\alpha_2}{g^2} + \dots$$

bringen. Darin bezeichnet g eine beliebige ganze Zahl, die größer als 1 ist, und $\alpha_0, \alpha_1, \alpha_2, \dots$ sind ganze Zahlen, die — abgesehen von α_0 — sämtlich kleiner als g sind. Auch von diesen Brüchen gilt der Satz, daß die Periode aus so viel Stellen besteht, wie der Exponent, zu welchem die Basis g für den Nenner als Modul gehört, Einheiten enthält. Da z. B. die Zahl 2 für die Moduln 3, 5, 7, 11 beziehungsweise zu den Exponenten 2, 4, 3, 10 gehört, so besteht im System der Basis 2 die Periode von $\frac{1}{3}$ aus 2, diejenige von $\frac{1}{5}$ aus 4, diejenige von $\frac{1}{7}$ aus 3, diejenige von $\frac{1}{11}$ aus zehn Ziffern. In der umstehenden Tabelle, die Material für hierher gehörige Aufgaben geben soll, ist über die jedesmalige Periode ein Strich gesetzt.

¹⁾ Berlin. Druck von A. W. Hayns Erben.

Ge- meiner Bruch	Entwicklung für die Basis					
	2	3	4	5	10	12
$\frac{1}{2}$	0,1	$0,1\bar{1} \dots$	0,2	0,22...	0,5	0,6
$\frac{1}{3}$	$0,0\bar{1}0 \dots$	0,1	$0,1\bar{1} \dots$	$0,1\bar{3}1 \dots$	$0,3\bar{3} \dots$	0,4
$\frac{1}{4}$	0,01	$0,0\bar{2}0 \dots$	0,1	0,11...	0,25	0,3
$\frac{1}{5}$	$0,001\bar{1}0 \dots$	$0,012\bar{1}0 \dots$	0,080...	0,1	0,2	$0,249\bar{7}2 \dots$
$\frac{1}{6}$	$0,00\bar{1}0 \dots$	0,011...	$0,0\bar{2}2 \dots$	$0,0\bar{4}0 \dots$	$0,1\bar{6}6 \dots$	0,2
$\frac{1}{7}$	$0,001\bar{0} \dots$	$0,010\bar{2}1\bar{2}0 \dots$	$0,0\bar{2}1\bar{0} \dots$	$0,0\bar{3}24\bar{1}20 \dots$	$0,1428\bar{5}71 \dots$	$0,186 \alpha 351 \dots ^1)$
$\frac{1}{8}$	0,001	$0,01\bar{0} \dots$	0,02	$0,0\bar{5}0 \dots$	0,125	0,16
$\frac{1}{9}$	$0,0001\bar{1}10 \dots$	0,01	$0,01\bar{5}0 \dots$	$0,0\bar{2}34\bar{2}10 \dots$	$0,1\bar{1} \dots$	0,14
$\frac{1}{10}$	$0,0001\bar{1}0 \dots$	$0,002\bar{2}0 \dots$	$0,012\bar{1} \dots$	$0,0\bar{2}2 \dots$	0,1	$0,1249\bar{7}2 \dots$
$\frac{1}{11}$	$0,00010111010 \dots$	$0,0021\bar{1}0 \dots$	$0,011\bar{3}10 \dots$	$0,0\bar{2}114\bar{0} \dots$	$0,0\bar{9}0 \dots$	$0,11 \dots$
$\frac{1}{12}$	$0,000\bar{1}0 \dots$	$0,002\bar{0} \dots$	$0,011 \dots$	$0,0\bar{2}0 \dots$	$0,08\bar{3}3 \dots$	0,1

¹⁾ $\alpha = \text{Zehn.}$

¹⁾ $\alpha = \text{Zehn.}$

§. 102.

Aufgaben.

I. Ein reduzierter Bruch hat zum Nenner 6075. Bei seiner Verwandlung in einen Kettenbruch hat der vorletzte Näherungsbruch den Nenner 2249. Welches ist der Bruch?

1. Lösung. Wir nehmen an, der Bruch sei $\frac{x}{6075}$, sein vorletzter Näherungsbruch $\frac{y}{2249}$. Dann ist

$$2249x - 6075y = +1 \quad \text{oder} \quad = -1,$$

je nachdem die Anzahl der unvollständigen Quotienten gerade oder ungerade ist. [Bekanntlich können wir den einen oder den anderen Fall nach Belieben herbeiführen, da wir den letzten unvollständigen Quotienten q , wenn die Anzahl der Quotienten um eine Einheit vergrößert werden soll, durch

$$(q - 1) + \frac{1}{1}$$

ersetzen können.] Die erste Annahme liefert $x \equiv 1799$, die zweite

$$x \equiv -1799 \equiv 4276 \pmod{6075}.$$

Die kleinsten Brüche, welche der Aufgabe genügen, sind also

$$\frac{1799}{6075} \quad \text{und} \quad \frac{4276}{6075}.$$

2. Lösung. Wir entwickeln — unter Anwendung der Bezeichnung des §. 59 — $\frac{Q}{Q_{n-1}}$ in einen Kettenbruch. Es ergibt sich

$$\frac{Q}{Q_{n-1}} = \frac{6075}{2249} = (2, 1, 2, 2, 1, 7, 1, 1, 1, 2, 3)$$

oder

$$= (2, 1, 2, 2, 1, 7, 1, 1, 1, 2, 2, 1).$$

Zur Kenntnis des Bruches $\frac{P}{P_{n-1}}$ fehlt uns dann nur der letzte unvollständige Quotient α dieses Bruches. Die übrigen unvollständigen Quotienten von $\frac{P}{P_{n-1}}$ stimmen mit denjenigen

von $\frac{Q}{Q_{n-1}}$ ganz überein. Wir bilden jetzt die Näherungsbrüche von $\frac{Q}{Q_{n-1}}$ und von $\frac{P}{P_{n-1}}$, wobei wir der Kürze wegen nur den Schluß der Rechnung hinschreiben. Der erste Kettenbruch liefert

.....	3	α	
.....	$\frac{1799}{666}$	$\frac{6075}{2249}$	$\frac{6075\alpha + 1799}{2249\alpha + 666}$

der zweite

.....	2	1	α	
.....	$\frac{1799}{666}$	$\frac{4276}{1583}$	$\frac{6075}{2249}$	$\frac{6075\alpha + 4276}{2249\alpha + 1583}$

Wir erhalten also für den Zähler P des gesuchten Bruches

$$P \equiv 1799 \text{ oder } \equiv 4276 \pmod{6075},$$

somit dasselbe Resultat wie bei der ersten Lösung.

II. Welche Gleichung hat als Wurzel den Kettenbruch

$$(0, \overline{1, 2, 5}, 1, \dots)?$$

Näherungsbrüche:

0	1	2	$5+x$	
$\frac{1}{0}$	$\frac{0}{1}$	$\frac{1}{1}$	$\frac{2}{3}$	$\frac{11+2x}{16+3x}$

Es is also

$$x = \frac{11+2x}{16+3x}$$

oder

$$3x^2 + 14x = 11.$$

III. Die kleinste Lösung der Gleichung

$$x^2 - 70x = 1$$

zu ermitteln.

Es ist

$$\sqrt{70} = (8, \overline{2, 1, 2, 1, 2, 16, 2, \dots}).$$

Näherungsbrüche:

8	2	1	2	1	2	16
$\frac{1}{0}$	$\frac{8}{1}$	$\frac{17}{2}$	$\frac{25}{3}$	$\frac{67}{8}$	$\frac{92}{11}$	$\frac{251}{30}$

Lösung:

$$x = 251, \quad y = 30.$$

IV. Welchen Rest giebt 7^{53} bei der Division durch 81?

$$7^{53} \equiv x \pmod{81},$$

$$53 \text{ Ind. } 7 \equiv \text{Ind. } x \pmod{54},$$

$$53 \cdot 16 \equiv \text{Ind. } x \pmod{54},$$

$$\text{Ind. } x \equiv 848 \equiv 38 \pmod{54},$$

$$x \equiv 58 \pmod{81}.$$

V. $2^x \equiv 13 \pmod{17},$

$$14x \equiv 4 \pmod{16},$$

$$7x \equiv 2 \pmod{8},$$

$$x \equiv 6 \pmod{8},$$

$$x \equiv 6 \text{ oder } \equiv 14 \pmod{16},$$

$$x = 6 + 16k \text{ oder } 14 + 16k.$$

VI. Eine Zahl hat rechts eine 4. Wird diese 4 rechts abgeschnitten und links angesetzt, so erhält man eine Zahl, die sich zur ursprünglichen wie 3:2 verhält. Welches ist die Zahl?

Lösung. Wird die Zahl $= 10a + 4$ gesetzt, so soll

$$(10a + 4) : (4 \cdot 10^x + a) = 2:3$$

sein. Daraus folgt

$$8 \cdot 10^x + 2a = 30a + 12,$$

$$2 \cdot 10^x = 7a + 3,$$

$$2 \cdot 10^x \equiv 3 \pmod{7},$$

$$2 + x \equiv 1 \pmod{6},$$

$$x \equiv -1 \equiv 5 \pmod{6}.$$

Der kleinste Wert von x ist also 5; für diesen ergibt sich

$$a = \frac{2 \cdot 10^5 - 3}{7} = \frac{199997}{7} = 28571;$$

somit ist die Zahl 285714.

VII. Die Zahlen

$$5^7 + 1, \quad 5^8 + 1, \quad 5^9 + 1$$

in Faktoren zu zerlegen.

Man erhält

$$5^7 + 1 = 2 \cdot 3 \cdot 29 \cdot 449,$$

$$5^8 + 1 = 2 \cdot 17 \cdot 11489,$$

$$5^9 + 1 = 2 \cdot 3^3 \cdot 7 \cdot 5167.$$

[Der Faktor 7 im letzten Beispiel rührt daher, daß

$$5^9 + 1 = 125^3 + 1$$

und 7 ein Divisor von 126 ist.]

VIII. Die Zahl

$$5^9 - 1 = 1953124 = 4 \cdot 488281$$

in Faktoren zu zerlegen.

Um den Lehrsatz II des §. 99 anwenden zu können, schreiben wir $5^9 - 1 = 125^3 - 1$. Dann muß eine in die vorgelegte Zahl aufgehende ungerade Primzahl entweder die Form $6k + 1$ haben oder in $124 = 4 \cdot 31$ aufgehen. Man erhält zunächst

$$5^9 - 1 = 4 \cdot 31 \cdot 15751.$$

Die Primzahlen der Form $6k + 1$ sind

$$7, 13, 19, 31, \dots,$$

und da $15751 = 19 \cdot 829$ und 829 eine Primzahl ist, so ergibt sich

$$5^9 - 1 = 4 \cdot 31 \cdot 19 \cdot 829.$$

IX. Wieviel Stellen hat die Periode des Dezimalbruches, den die Entwicklung von $\frac{1}{42471}$ liefert? Da

$$42471 = 3^3 \cdot 11^2 \cdot 13$$

ist, so erfordert die Lösung der Kongruenz

$$10^x \equiv 1 \pmod{42471}$$

diejenige der drei Kongruenzen

$$10^{x_1} \equiv 1 \pmod{3^3}, \quad 10^{x_2} \equiv 1 \pmod{11^2}, \quad 10^{x_3} \equiv 1 \pmod{13}.$$

Die erste und die dritte können ohne weiteres mittels der Indizestafeln des Anhangs gelöst werden. Man erhält

$$x_1 \equiv 0 \pmod{3}, \quad x_3 \equiv 0 \pmod{6}.$$

Was die zweite Kongruenz betrifft, so ist nach §. 91, Beispiel II 2 die kleinste primitive Wurzel von 121, und durch Ausrechnung der Potenzreste von 2 findet man

$$2^{20} \equiv -10 \pmod{121}.$$

Da nun noch

$$\frac{1}{2} \varphi(121) = 55,$$

also

$$2^{55} \equiv -1 \pmod{121}$$

ist, so erhält man

$$2^{75} \equiv (-10)(-1) \equiv 10 \pmod{121},$$

folglich ist

$$\text{Ind. } 10 \equiv 75 \pmod{110}.$$

Bei Benutzung dieses Wertes liefert die zweite Kongruenz

$$75 x_2 \equiv 0 \pmod{110},$$

$$15 x_2 \equiv 0 \pmod{22},$$

$$x_2 \equiv 0 \pmod{22}.$$

Die gesuchte Zahl x muß danach durch die Moduln 3, 6, 22, also durch 66 teilbar sein. Die kleinste Zahl, welche diesen Bedingungen genügt, ist 66, und somit besteht die Periode des vorgelegten Bruches aus 66 Ziffern. Dasselbe Resultat hätte die Tabelle von Gauss geliefert.

X. Die Brüche $\frac{1}{17}$ und $\frac{1}{18}$ in Duodezimalbrüche zu verwandeln.

Man erhält, wenn $\alpha = \text{zehn}$, $\beta = 11$ ist,

$$\frac{1}{17} = 0,08579214\beta 36429\alpha 70 \dots, \quad \frac{1}{18} = 0,08.$$

XI. Zu beweisen, daß

$$a^{(p-1)p^2-1} - b^{(p-1)p^2-1}$$

durch p^2 teilbar ist, wenn die Primzahl p weder in a noch in b aufgeht.

XII. Für welche Basis g ist

$$\frac{1}{2} = 0,\overline{77} \dots?$$

Aus

$$\frac{7}{g} + \frac{7}{g^2} + \dots = \frac{1}{2}$$

folgt

$$\frac{\frac{7}{g}}{1 - \frac{1}{g}},$$

d. i.

$$\frac{7}{g-1} = \frac{1}{2}.$$

Es ist also

$$g - 1 = 14, \text{ folglich } g = 15.$$

XIII. Für welche Basis ist ebenso

$$\frac{2}{5} = 0,\overline{121} \dots?$$

Man erhält $g = 4$.

Achtes Kapitel.

Kongruenzen zweiten Grades.

§. 103.

Auflösung der rein quadratischen Kongruenz.

Die Kongruenz

$$x^2 \equiv a \pmod{m}$$

ist eine binomische Kongruenz zweiten Grades und als solche schon in §. 79 (für $m = p$), §. 94 ($m = p^2$ oder $2p^2$), §. 97 (für $m = 2^2$) und §. 98 (für $m = 2^2 p^2 q^\mu \dots$) behandelt worden. Auch wird sie uns in der Folge noch eingehend beschäftigen. Zum besseren Verständnis der nachstehenden Entwicklungen wird es aber hin und wieder schon vorher nötig sein, die Wurzeln einer solchen Kongruenz zu bestimmen. Deshalb soll hier ein einfaches Probiervverfahren gelehrt werden, welches diese Wurzeln in den meisten Fällen schnell liefert. Dasselbe besteht darin, daß man die Reihe

$$a, a + m, a + 2m, \dots$$

bildet und sich die Quadratzahlen merkt, die in derselben vorkommen. Jede dieser Quadratzahlen μ^2 liefert ein Wurzelpaar $\pm \mu$ der Kongruenz $x^2 \equiv a \pmod{m}$.

Die Frage, wie weit man die Reihe fortzuführen hat, um alle Wurzeln zu erhalten, wird bei der späteren Behandlung des Verfahrens ihre Erledigung finden. Hier sei nur im voraus mitgeteilt, daß man sich, um alle Wurzeln zu finden, im all-

gemeinen auf die ersten $E\left(\frac{m}{4}\right)$ Glieder beschränken kann, wo $E\left(\frac{m}{4}\right)$ die größte in dem Bruche $\frac{m}{4}$ enthaltene ganze Zahl bezeichnet.

Sollen z. B. alle Wurzeln der Kongruenz $x^2 \equiv 1 \pmod{40}$ gefunden werden, so bilde man die Reihe

$$1, 41, 81, 121, 161, 201, 241, 281, 321, 361.$$

In derselben befinden sich die vier Quadratzahlen 1, 81, 121, 361; folglich hat die Kongruenz die acht Wurzeln

$$\pm 1, \pm 9, \pm 11, \pm 19.$$

§. 104.

Verwandlung der gemischt quadratischen Kongruenz mit einer Unbekannten in eine rein quadratische.

Die allgemeine Kongruenz zweiten Grades mit einer Unbekannten hat die Form

$$(1) \quad ax^2 + bx + c \equiv 0 \pmod{m};$$

darin bezeichnen a, b, c ganze Zahlen, von denen weder a noch c durch m teilbar sein kann, da die Kongruenz sonst aufhören würde, vom zweiten Grade zu sein. Dagegen kann $b \equiv 0 \pmod{m}$ sein. In diesem Falle ist die Kongruenz eine rein quadratische.

Wir setzen jetzt voraus, daß keiner der Koeffizienten a, b, c durch den Modul m teilbar ist, und wollen zeigen, wie man dann die Kongruenz in eine rein quadratische verwandelt, deren erstes Glied zugleich den Koeffizienten 1 hat.

I. Wenn a prim zum Modul m ist, so können wir nach §. 40 eine Zahl α bestimmen, welche der Bedingung

$$a\alpha \equiv 1 \pmod{m}$$

genügt. Die Zahl α wird augenscheinlich ebenfalls prim zu m sein. Durch Multiplikation der vorgelegten Kongruenz mit α ergibt sich dann

$$(2) \quad x^2 + b\alpha x + c\alpha \equiv 0 \pmod{m}.$$

[Der Modul bleibt m , eben weil α prim zu m ist.]

Wenn nun erstens $b\alpha$ eine gerade Zahl ist, die mit 2β bezeichnet werden möge, so ersetzen wir (2) durch

$$x^2 + 2\beta x + \beta^2 + c\alpha - \beta^2 \equiv 0 \pmod{m},$$

d. i.

$$(3) \quad (x + \beta)^2 + (c\alpha - \beta^2) \equiv 0 \pmod{m},$$

und auf diese Weise haben wir eine rein quadratische Kongruenz mit der Unbekannten $x + \beta$ erhalten (Beispiele I und II).

Wenn zweitens $b\alpha$ zwar ungerade, zugleich aber auch m ungerade ist, so können wir $b\alpha$ durch die kongruente gerade Zahl $-(m - b\alpha)$ ersetzen und dann verfahren, wie eben gezeigt worden ist (Beispiel III).

Wenn drittens $b\alpha$ ungerade und zugleich m gerade ist, also eine Kongruenz der Form

$$(4) \quad x^2 + (2\beta + 1)x + c \equiv 0 \pmod{2\mu}$$

vorliegt, so erhalten wir durch Multiplikation mit 4

$$4x^2 + 4(2\beta + 1)x + 4c \equiv 0 \pmod{8\mu}$$

oder

$$[2x + (2\beta + 1)]^2 + [4c - (2\beta + 1)^2] \equiv 0 \pmod{8\mu},$$

und das ist eine rein quadratische Kongruenz mit der Unbekannten $2x + (2\beta + 1)$ (Beispiel IV).

II. Es sei jetzt a nicht prim zum Modul m . Dann läßt sich der Koeffizient von x^2 in der Kongruenz (1) nicht auf die Einheit reduzieren.

Wenn nun erstens b eine gerade Zahl 2β ist oder sich durch eine kongruente gerade Zahl ersetzen läßt, was im Falle eines ungeraden Moduls stets möglich ist, so erhalten wir durch Multiplikation der Kongruenz (1) mit a

$$a^2 x^2 + 2\beta a x + c a \equiv 0 \pmod{a m}$$

oder

$$(5) \quad (ax + \beta)^2 + (ca - \beta^2) \equiv 0 \pmod{a m},$$

und das ist eine rein quadratische Kongruenz mit der Unbekannten $ax + \beta$ (Beispiel V).

Wenn zweitens b ungerade ist und sich auch nicht durch eine kongruente gerade Zahl ersetzen läßt (der Modul ist in diesem Falle gerade), so haben wir mit $4a$ zu multiplizieren. Dadurch erhalten wir

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{4am}$$

oder

$$(6) \quad (2ax + b)^2 + (4ac - b^2) \equiv 0 \pmod{4am},$$

und das ist ebenfalls eine rein quadratische Kongruenz; ihre Unbekannte ist $2ax + b$ (Beispiel VI).

Man kann also eine gemischt quadratische Kongruenz immer durch eine rein quadratische ersetzen. Nach Auflösung der letzteren, d. i. nach Bestimmung der Werte der neuen Unbekannten, hat man dann noch die Werte der ursprünglichen Unbekannten x zu suchen.

Beispiele. I. Die Kongruenz

$$5x^2 - 11x - 12 \equiv 0 \pmod{23}$$

geht durch Multiplikation mit 14 über in

$$70x^2 - 154x - 168 \equiv 0 \pmod{23}$$

oder

$$x^2 - 16x - 7 \equiv 0 \pmod{23}.$$

Es ist also

$$(x - 8)^2 - 7 - 64 \equiv 0 \pmod{23}$$

oder

$$(x - 8)^2 \equiv 2 \pmod{23}.$$

Die Reihe 2, 25, ... enthält die Quadratzahl 25^1 ; es ist also

$$x - 8 \equiv +5 \quad \text{und} \quad \equiv -5,$$

folglich

$$x \equiv +13 \quad \text{und} \quad \equiv +3 \pmod{23}.$$

$$\text{II. } 3x^2 + 4x + 5 \equiv 0 \pmod{20},$$

$$21x^2 + 28x + 35 \equiv 0,$$

$$x^2 + 8x + 15 \equiv 0,$$

$$(x + 4)^2 + 15 - 16 \equiv 0,$$

$$(x + 4)^2 \equiv 1 \pmod{20}.$$

Die Reihe

$$1, 21, 41, 61, 81$$

enthält die Quadratzahlen 1 und 81, folglich ist

$$x + 4 \equiv +1, -1, +9, -9,$$

also

$$x \equiv -3, -5, +5, -13 \pmod{20}.$$

¹⁾ Da der Modul 23 eine Primzahl ist, so giebt es, wie wir später sehen werden, nur ein Wurzepaar. Man darf also die Reihe abbrechen, sobald eine Quadratzahl erscheint.

$$\text{III. } 7x^2 - 3x + 11 \equiv 0 \pmod{19},$$

$$77x^2 - 33x + 121 \equiv 0,$$

$$x^2 - 14x + 7 \equiv 0,$$

$$(x - 7)^2 \equiv 42 \equiv 4,$$

$$x - 7 \equiv +2, -2,$$

$$x \equiv +9, +5 \pmod{19}.$$

$$\text{IV. } 5x^2 - 3x - 2 \equiv 0 \pmod{12},$$

$$25x^2 - 15x - 10 \equiv 0,$$

$$x^2 - 3x + 2 \equiv 0,$$

$$4x^2 - 12x + 8 \equiv 0 \pmod{48},$$

$$(2x - 3)^2 \equiv 1 \pmod{48}.$$

Die Reihe

1, 49, 97, 145, 193, 241, 289, 337, 385, 433, 481, 529

enthält die Quadratzahlen 1, 49, 289, 529, folglich ist mod. 48

$2x - 3 \equiv +1$	-1	$+7$	-7	$+17$	-17	$+23$	-23
$2x \equiv 4$	2	10	-4	20	-14	26	-20
$x \equiv 2$	1	5	-2	10	-7	13	-10

Da nun mod. 12

$$10 \equiv -2, -7 \equiv 5, 13 \equiv 1, -10 \equiv 2$$

ist, so besitzt die vorgelegte Kongruenz nur die vier Wurzeln

$$x \equiv 1, \pm 2, 5 \pmod{12}.$$

$$\text{V. } 3x^2 + 4x + 9 \equiv 0 \pmod{12},$$

$$9x^2 + 12x + 27 \equiv 0 \pmod{36},$$

$$(3x + 2)^2 \equiv -23 \equiv 13 \pmod{36}.$$

Die Reihe

13, 49, 85, 121, 157, 193, 229, 265, 301

enthält die Quadratzahlen 49 und 121, folglich ist (mod. 36)

$3x + 2 \equiv +7$	-7	$+11$	-11
$3x \equiv 5$	-9	$+9$	-13
$x \equiv$	-3	$+3$	

Die vorgelegte Kongruenz besitzt also die beiden Wurzeln

$$x \equiv \pm 3 \pmod{12}.$$

$$\begin{aligned} \text{VI. } 3x^2 + x - 4 &\equiv 0 \pmod{10}, \\ 36x^2 + 12x - 48 &\equiv 0 \pmod{120}, \\ (6x + 1)^2 &\equiv 49 \pmod{120}. \end{aligned}$$

Die Reihe

49, 169, 289, 409, 529, 649, 769, 889, 1009, 1129, 1249, 1369,
1489, 1609, 1729, 1849, 1969, 2089, 2209, 2329, 2449, 2569,
2689, 2809, 2929, 3049, 3169, 3289, 3409, 3529

enthält die Quadratzahlen 49, 169, 289, 529, 1369, 1849, 2209,
2809, folglich ist $\pmod{120}$

$6x + 1 \equiv +7$	-7	$+13$	-13	$+17$	-17	$+23$	-23
$6x \equiv 6$	-8	$+12$	-14	$+16$	-18	$+22$	-24
$x \equiv 1$		$+2$			-3		-4

$6x + 1 \equiv +37$	-37	$+43$	-43	$+47$	-47	$+53$	-53
$6x \equiv +36$	-38	$+42$	-44	$+46$	-48	$+52$	-54
$x \equiv +6$		$+7$			-8		-9

Nun ist aber $\pmod{10}$

$$-8 \equiv 2, \quad -9 \equiv 1, \quad -4 \equiv 6, \quad -3 \equiv 7,$$

folglich hat die vorgelegte Kongruenz die vier Wurzeln

$$x \equiv 1, 2, 6, 7 \pmod{10}.$$

§. 105.

Quadratische Reste und Nichtreste (Euler, *Commentationes arithmet. collectae* I, p. 477 ff.).

Wir haben in §. 104 gesehen, daß jede Kongruenz zweiten Grades mit einer Unbekannten auf die Form

$$x^2 \equiv a \pmod{m}$$

gebracht werden kann. Man kann sich nun leicht überzeugen, daß diese letztere Kongruenz bei gegebenem Modul m nicht für alle Werte von a möglich ist. Bilden wir nämlich die Reste, welche die Quadrate der Zahlen 0, 1, 2, 3, ... für den Modul m

geben, so können wir uns, da die Quadrate kongruenter Zahlen kongruent sind, auf die Zahlen

$$(1) \quad 0, 1, 2, 3, \dots, (m-1)$$

beschränken. Nun ist für jeden Wert von k

$$(m-k)^2 = m^2 - 2mk + k^2 \equiv k^2 \pmod{m};$$

folglich bilden die Quadrate der Zahlen (1), wenn man das erste Glied (Null) wegläßt, das sind die Zahlen

$$(2) \quad 1, 4, 9, \dots, 9, 4, 1$$

eine Reihe, in der jedenfalls die von den Enden gleich weit entfernten Glieder einander gleich sind. Es werden also, während einige der Zahlen (1) sich in (2) mehrmals vorfinden, andere gar nicht vorhanden sein.

So enthält für $m = 7$ die Reihe (1) die Zahlen 0, 1, 2, 3, 4, 5, 6; die Reihe (2), welche die Reste der Quadrate der Zahlen von 1 bis 6 giebt, wird 1, 4, 2, 2, 4, 1 sein. Während also in (2) jede der Zahlen 1, 2, 4 zweimal erscheint, kommen 3, 5, 6 gar nicht vor.

Für den Modul 12 wird die Reihe (2)

$$1, 4, 9, 4, 1, 0, 1, 4, 9, 4, 1$$

sein; es fehlen also die Zahlen

$$2, 3, 5, 6, 7, 8, 10, 11.$$

Danach ist die Kongruenz $x^2 \equiv 2 \pmod{7}$ möglich; ihre Wurzeln sind ± 3 . Ebenso ist die Kongruenz $x^2 \equiv 1 \pmod{12}$ möglich; sie hat die vier Wurzeln $\pm 1, \pm 5$. Dagegen sind die Kongruenzen

$$x^2 \equiv 3 \pmod{7}, \quad x^2 \equiv 2 \pmod{12}$$

unmöglich, d. h. es giebt keine ganze Zahl, deren Quadrat für den Modul 7 den Rest 3 oder für den Modul 12 den Rest 2 liefert.

Die Zahlen

$$0, 1, 2, 3, \dots, m-1$$

und somit alle Zahlen lassen sich danach in zwei Klassen teilen. Die erste Klasse umfaßt alle diejenigen Zahlen a , die einer Quadratzahl für den Modul m kongruent sind, für die also die Kongruenz $x^2 \equiv a \pmod{m}$ möglich ist. Die zweite Klasse enthält alle diejenigen Zahlen, die keiner Quadratzahl für den

Modul m kongruent sind, für die also die Kongruenz

$$x^2 \equiv a \pmod{m}$$

unmöglich ist. Die Zahlen der ersten Klasse heißen die quadratischen Reste von m , die Zahlen der zweiten Klasse die quadratischen Nichtreste von m . Wo kein Mißverständnis zu befürchten ist, sagt man einfach Reste und Nichtreste. Der Modul 7 hat also die Reste 0, 1, 2, 4, die Nichtreste 3, 5, 6; der Modul 12 hat die Reste 0, 1, 4, 9, die Nichtreste 2, 3, 5, 6, 7, 8, 10, 11.

Anmerkungen. I. Da 2, 3, 7, 8 Nichtreste von 10 sind, so kann eine dekadisch geschriebene Zahl, wenn sie auf eine dieser Ziffern endigt, keine Quadratzahl sein. Dies war schon den Mathematikern des 11. und 12. Jahrhunderts bekannt, so dem Alkarkhî (Kâfi fil Hisâb, übersetzt von A. Hochheim, II, S. 13), dem Abraham ibn Esra (Sefer Ha-Mispar, übersetzt von M. Silberberg, S. 66). Nicolas Chuquet erwähnt die Thatsache in seinem 1484 abgefaßten Werke *Triparty en la Science des Nombres* (Ausgabe von Aristide Marre, p. 108). Alkarkhî und Ibn Esra geben l. c. auch 0, 1, 4, 7 als quadratische Reste von 9 an.

II. Bei der Berechnung der quadratischen Reste bedient man sich mit Vorteil der Formel

$$(n - 1)^2 + (2n - 1) = n^2,$$

schreibt also z. B., wenn die Reste von 23 gefunden werden sollen,

$$\begin{aligned} 1, \quad 1 + 3 = 4, \quad 4 + 5 = 9, \quad 9 + 7 = 16, \quad 16 + 9 = 25 \equiv 2, \\ 2 + 11 = 13, \quad 13 + 13 \equiv 3, \quad 3 + 15 = 18, \quad 18 + 17 \equiv 12, \\ 12 + 19 \equiv 8, \quad 8 + 21 \equiv 6. \end{aligned}$$

Die Reste von 23 sind also

$$0, 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18,$$

die Nichtreste

$$5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22.$$

III. Der Einfachheit wegen schließen wir im Folgenden die Zahl 0, welche immer Rest ist, und die Zahlen, welche nicht prim zum Modul sind, von der Betrachtung vorläufig aus.

§. 106.

Reste einer ungeraden Primzahl.

Für die (einzige) gerade Primzahl 2 ist 1 quadratischer Rest, ein Nichtrest ist nicht vorhanden. Für die ungeraden Primzahlen gilt der

Lehrsatz. Wenn der Modul p eine ungerade Primzahl ist, so enthält die Reihe

$$1, 2, 3, \dots, p-1$$

$\frac{p-1}{2}$ Reste und ebenso viele Nichtreste.

Beweis. Wir zeigen, daß die Quadrate der Zahlen

$$1, 2, 3, \dots, \frac{p-1}{2}$$

für den Modul p nicht kongruent sein können. Wären a und $b < a$ zwei dieser Zahlen, und hätte man

$$a^2 \equiv b^2, \text{ also } a^2 - b^2 \equiv 0,$$

d. i.

$$(a+b)(a-b) \equiv 0 \pmod{p},$$

so müßte, da p eine Primzahl ist, entweder $a+b$ oder $a-b$ durch p teilbar sein. Das ist aber unmöglich; denn da jede der Zahlen a, b kleiner als $\frac{p}{2}$ sein soll, so ist sowohl $a+b$, als auch $a-b$ kleiner als p , und da $a > b$ vorausgesetzt wird, so ist $a-b$ von Null verschieden. Die Quadrate der ersten Hälfte der Zahlen

$$1, 2, 3, \dots, p-1$$

sind also inkongruent. Die Quadrate der folgenden Zahlen

$$\frac{p+1}{2}, \frac{p+3}{2}, \dots, p-1$$

liefern aber wieder dieselben Reste wie die Quadrate der Zahlen

$$1, 2, 3, \dots, \frac{p-1}{2}$$

und zwar in umgekehrter Reihenfolge; denn es ist, wenn

$$p = 2n + 1$$

gesetzt wird, die erste Hälfte der in Betracht kommenden Zahlen

$$1, 2, 3, \dots, n,$$

die zweite Hälfte

$$n + 1, n + 2, \dots, 2n,$$

und man hat

$$(n + 1)^2 = n^2 + (2n + 1) = n^2 + p \equiv n^2 \pmod{p},$$

$$(n + 2)^2 = (n - 1)^2 + 3(2n + 1) = (n - 1)^2 + 3p \equiv (n - 1)^2.$$

$$\dots \dots \dots$$

$$(2n)^2 = 1^2 + (2n - 1)(2n + 1) = 1^2 + (2n - 1)p \equiv 1^2 \pmod{p}.$$

Somit sind unter den Zahlen

$$1, 2, 3, \dots, p - 1,$$

also auch in jedem vollständigen Restsysteme des Moduls p ebenso

viele Reste wie Nichtreste, d. i. $\frac{p-1}{2}$ Zahlen jeder der beiden Arten vorhanden.

Über die Wurzeln der Kongruenz $x^2 \equiv a \pmod{p}$.

Wenn ξ eine Wurzel der Kongruenz $x^2 \equiv a \pmod{p}$ bezeichnet, so ist auch $-\xi$ eine Wurzel derselben; denn es ist

$$(-\xi)^2 \equiv \xi^2 \pmod{p},$$

und $-\xi$ kann nicht $+\xi$ kongruent sein, da sonst die Differenz beider Zahlen, d. i. 2ξ , durch p teilbar sein müßte, was die Teilbarkeit von ξ durch p erfordern würde. Die Kongruenz hat dann also die beiden Wurzeln $\pm \xi$, und da sie nach §. 47, Lehrsatz I nicht mehr als zwei Wurzeln haben kann, so sind $\pm \xi$ ihre einzigen Wurzeln.

Anmerkung. Wir lassen hier die Zahlen von 1 bis $p-1$ für jeden der beiden Moduln

$$p = 17, \quad p = 19$$

folgen; dabei ist zur Veranschaulichung unter jeden Rest das Zeichen $+$, unter jeden Nichtrest das Zeichen $-$ gesetzt.

I. mod. 17.

1	2	3	4	5	6	7	8
+	+	-	+	-	-	-	+
16	15	14	13	12	11	10	9
+	+	-	+	-	-	-	+

II. mod. 19.

1	2	3	4	5	6	7	8	9
+	—	—	+	+	+	+	—	+
18	17	16	15	14	13	12	11	10
—	+	+	—	—	—	—	+	—

Aus diesen Beispielen entnehmen wir den Satz, der in §. 115 bewiesen werden soll:

Wenn die Primzahl p die Form $4n + 1$ hat, so sind zwei einander zum Modul ergänzende Zahlen beide Reste oder beide Nichtreste. Hat dagegen der Modul die Form $4n + 3$, so ist von zwei Zahlen, die einander zum Modul ergänzen, die eine ein Rest, die andere ein Nichtrest.

Da nun $+1$ ein Rest für jede Primzahl ist, so würde sich aus dem vorhergehenden Satze weiter ergeben:

Für die Primzahlen p der Form $4n + 1$ ist

$$p - 1 \equiv -1$$

ein Rest, für die Primzahlen der Form $4n + 3$ ein Nichtrest.

§. 107.

Reste einer Potenz einer ungeraden Primzahl.

Lehrsatz I. Unter den $\varphi(p^2)$ Zahlen, welche prim zu p^2 und kleiner als p^2 sind, befinden sich ebenso viele Reste wie Nichtreste von p^2 .

Beweis. Wenn die Zahl a prim zu p^2 ist, so ist es auch $p^2 - a$, und wenn

$$a < \frac{1}{2} p^2$$

ist, so ist

$$p^2 - a > \frac{1}{2} p^2.$$

Daher ist die Hälfte der Zahlen, die prim zu p^2 und $< p^2$ sind kleiner, die andere Hälfte größer als $\frac{1}{2} p^2$.

Es soll nun gezeigt werden, daß die Quadrate der einen Hälfte, etwa der Zahlen, die $< \frac{1}{2} p^2$ sind, nicht kongruent sein können. Es seien a und $b < a$ zwei solche Zahlen. Wäre dann

$$a^2 \equiv b^2, \text{ also } a^2 - b^2 \equiv 0,$$

d. i.

$$(a + b)(a - b) \equiv 0 \pmod{p^2},$$

so müßte entweder eine der Zahlen $a + b$, $a - b$ durch p^2 teilbar sein, oder es müßte $a + b$ durch eine Potenz p^k (wo $k < 2$ wäre) und $a - b$ durch p^{2-k} , also jedenfalls sowohl $a + b$ als auch $a - b$ durch p teilbar sein. Beides ist aber unmöglich. Da nämlich

$$a < \frac{1}{2} p^2, \quad b < \frac{1}{2} p^2$$

vorausgesetzt wird, so ist sowohl $a + b$, als auch $a - b$ kleiner als p^2 ; ferner ist $a - b$ von Null verschieden, denn b soll $< a$ sein. Somit ist weder $a + b$, noch $a - b$ durch p^2 teilbar. Wäre ferner jede der beiden Zahlen $a + b$, $a - b$ durch p teilbar, so müßte auch ihre Summe, d. i. $2a$, und ebenso ihre Differenz, d. i. $2b$, durch p teilbar sein; da aber 2 prim zu p ist, so würde das erfordern, daß sowohl a als auch b durch p teilbar wäre, während a und b prim zu p sein sollen. Die Quadrate der $\frac{1}{2} \varphi(p^2)$ Zahlen, welche prim zu p und $< \frac{1}{2} p^2$ sind, sind also in der That inkongruent, und somit haben wir $\frac{1}{2} \varphi(p^2)$ quadratische Reste von p^2 erhalten.

Noch andere quadratische Reste besitzt aber p^2 nicht; denn die zweite Hälfte der Zahlen, die prim zu p^2 und $< p^2$ sind, liefert wieder (in umgekehrter Reihenfolge) dieselben Reste wie die erste Hälfte, da allgemein

$$(p^2 - a)^2 = p^2 - 2ap^2 + a^2 \equiv a^2 \pmod{p^2}$$

ist. Somit ist die Zahl der Reste wie die der Nichtreste gleich

$$\frac{1}{2} \varphi(p^2) = \frac{1}{2} (p - 1)p^{2-1}.$$

Lehrsatz II. Jeder Rest von p ist auch Rest von p^2 , jeder Nichtrest von p Nichtrest von p^2 .

Beweis. Der zweite Teil des Satzes leuchtet ohne weiteres ein. Wenn nämlich die Kongruenz

$$x^2 \equiv a \pmod{p}$$

unmöglich ist, so läßt sich auch kein Wert von x finden, für welchen $x^2 - a$ durch p^2 teilbar wäre. Somit ist jeder Nichtrest von p auch Nichtrest von p^2 , und wir haben die Reste von p^2 nur unter den Resten von p zu suchen.

Nun lassen sich die $\varphi(p^2) = (p-1)p$ Zahlen, welche prim zu p und $< p^2$ sind, folgendermaßen in p Reihen schreiben:

$$\begin{array}{ccccccc} 1, & 2, & 3, & \dots, & p-1, \\ p+1, & p+2, & p+3, & \dots, & 2p-1, \\ \dots & \dots & \dots & \dots & \dots \\ p^2-p+1, & p^2-p+2, & p^2-p+3, & \dots, & p^2-1. \end{array}$$

Da jede dieser Reihen ein vollständiges Restsystem für den Modul p bildet, so enthält sie $\frac{p-1}{2}$ Reste von p ; es sind also

in den p Reihen im ganzen $\frac{1}{2}(p-1)p$ Reste von p vorhanden, und ebenso groß ist die Anzahl der Reste von p^2 . Wenn nun ein einziger jener Reste von p Nichtrest von p^2 wäre, so müßte es einen Rest von p^2 geben, der Nichtrest von p wäre, und das ist oben als unmöglich bewiesen worden. Somit ist auch jeder Rest von p ein Rest von p^2 .

Anmerkung. Auch hier lasse ich für zwei Moduln p^2 die Zahlen, welche prim zu p^2 und $< p^2$ sind (für den ersten ist $p = 4n+1$, für den zweiten $4n+3$), folgen und setze unter jede Zahl das Zeichen + oder —, jenachdem sie Rest oder Nichtrest des betreffenden Moduls ist.

I. mod. 25.

1	2	3	4	6	7	8	9	11	12
+	—	—	+	+	—	—	+	+	—
24	23	22	21	19	18	17	16	14	13
+	—	—	+	+	—	—	+	+	—

II. mod. 27.

1	2	4	5	7	8	10	11	13
+	—	+	—	+	—	+	—	+
26	25	23	22	20	19	17	16	14
—	+	—	+	—	+	—	+	—

Aufgabe. Aus der Wurzel α der Kongruenz

$$(1) \quad x^2 \equiv a \pmod{p^2}$$

eine Wurzel der Kongruenz

$$(2) \quad x^2 \equiv a \pmod{p^{2+1}}$$

herzuleiten.

Lösung. Da α eine Wurzel von (1) ist, so wird $\alpha + kp^2$ für jeden Wert von k der Kongruenz (1) genügen. Wir wollen jetzt über die unbestimmte Größe k so verfügen, daß $\alpha + kp^2$ eine Wurzel von (2) werde, daß also

$$(\alpha + kp^2)^2 \equiv a \pmod{p^{2+1}}$$

sei. Durch Entwicklung der linken Seite folgt

$$\alpha^2 + 2k\alpha p^2 + k^2 p^4 \equiv a \pmod{p^{2+1}},$$

oder, da $2k$ jedenfalls nicht kleiner als $2 + 1$ ist,

$$2k\alpha p^2 \equiv a - \alpha^2 \pmod{p^{2+1}}.$$

Nun ist α eine Wurzel von (1), also $a - \alpha^2$ durch p^2 teilbar. Wenn wir

$$a - \alpha^2 = \beta \cdot p^2$$

annehmen und die letzte Kongruenz durch p^2 dividieren, so erhalten wir

$$2k\alpha \equiv \beta \pmod{p}.$$

2α ist prim zu p ; folglich ist diese Kongruenz stets möglich und liefert für jedes α einen Wert von k ; jeder Wurzel von (1) entspricht also eine Wurzel von (2), und diese letztere ist bekannt, sobald man k bestimmt hat.

Nach §. 106 hat die Kongruenz

$$x^2 \equiv a \pmod{p}$$

zwei verschiedene Wurzeln; jede derselben liefert eine Wurzel von

$$x^2 \equiv a \pmod{p^2},$$

jede der letzteren ebenso eine Wurzel von

$$x^2 \equiv a \pmod{p^3},$$

u. s. w. Die Kongruenz

$$x^2 \equiv a \pmod{p^2}$$

hat also in jedem Falle zwei verschiedene Wurzeln, wofern nur a ein quadratischer Rest von p ist.

Beispiele: I. Die Kongruenz $x^2 \equiv 5$ hat für den

Modul	11	11 ²	11 ³	11 ⁴
die Wurzeln	± 4	± 48	± 73	± 6582 .

II. Die Kongruenz $x^2 \equiv 2$ hat für den

Modul	7	7 ²	7 ³	7 ⁴
die Wurzeln	$+ 3$	± 10	± 108	± 235 .

III. Die Kongruenz $x^2 \equiv -1$ hat für den

Modul	5	5 ²	5 ³	5 ⁴	5 ⁵
die Wurzeln	± 2	± 7	± 57	± 182	± 1068 .

§. 108.

Das Produkt aller Zahlen, die prim zu p^2 und $< p^2$ sind.

Da die Zahl $+1$ Rest von p^2 ist, so ist die Kongruenz

$$x^2 \equiv 1 \pmod{p^2}$$

möglich und hat zwei Wurzeln. Es sind dies die Zahlen $+1$ und $p^2 - 1 \equiv -1$; ihr Produkt ist

$$\equiv -1 \pmod{p^2}.$$

Was nun die übrigen $\varphi(p^2) - 2$ Zahlen betrifft, die prim zu p^2 und $< p^2$ sind, so lassen sich dieselben zu je zweien in der Weise zusammenstellen, daß das Produkt der beiden Zahlen jedes Paares

$$\equiv +1 \pmod{p^2}$$

ist. Bezeichnet nämlich a eine dieser $\varphi(p^2) - 2$ Zahlen, so ist die Kongruenz

$$ax \equiv 1 \pmod{p^2},$$

weil a prim zu p^2 ist, möglich und hat eine Wurzel ξ , die deshalb von a verschieden sein muß, weil sonst a eine Wurzel der

Kongruenz $x^2 \equiv 1 \pmod{p^2}$, also ± 1 sein müßte, was nicht der Fall sein soll. Ist b eine zweite jener Zahlen, so hat auch die Kongruenz $bx \equiv 1 \pmod{p^2}$ eine, aber auch nur eine Wurzel, die mit ξ' bezeichnet werden möge.

Wäre nun

$$\xi' = \xi \pmod{p^2},$$

so hätte man

$$b\xi' = b\xi = 1,$$

und da auch $a\xi = 1$ ist,

$$b\xi = a\xi \pmod{p^2}.$$

Diese Kongruenz könnte man durch ξ dividieren, und man erhielte, weil ξ prim zu p^2 ist,

$$a \equiv b \pmod{p^2},$$

während a und b als inkongruent vorausgesetzt werden.

Da das Produkt der Zahlen 1 und $p^2 - 1$ den Rest -1 liefert, das Produkt jedes Paares der übrigen Zahlen und daher auch das Produkt aller übrigen Zahlen den Rest $+1$, so ist das Produkt aller Zahlen, die prim zu p^2 und $< p^2$ sind,

$$\equiv -1 \pmod{p^2},$$

oder das um 1 vermehrte Produkt ist durch den Modul p^2 teilbar.

Anmerkung. Im Vorhergehenden ist der Wilsonsche Satz auf den Fall ausgedehnt, in welchem der Modul eine Potenz einer ungeraden Primzahl ist.

§. 109.

Eulers Kriterium zu entscheiden, ob eine Zahl Rest oder Nichtrest einer ungeraden Primzahl oder einer Potenz einer solchen sei (Euler, *Opuscula analytica* I, p. 263 = *Commentationes arithmet. collectae* II, p. 11).

Lehrsatz. Eine Zahl a ist Rest oder Nichtrest von p^2 , $\lambda \geq 1$, jenachdem

$$a^{\frac{1}{2}\varphi(p^2)} \equiv +1$$

oder

$$\equiv -1 \pmod{p^2}$$

ist.

Beweis. Es seien m und a zwei von den $\varphi(p^2)$ Zahlen, die prim zu p^2 und $< p^2$ sind. Dann hat die Kongruenz

$$mx \equiv a \pmod{p^2}$$

stets eine und nur eine Lösung. Diese Lösung kann erstens gleich m sein. Dann ist

$$m^2 \equiv a \pmod{p^2},$$

also a Rest von p^2 und m eine Wurzel der Kongruenz

$$x^2 \equiv a \pmod{p^2}.$$

Die zweite Wurzel wird $p^2 - m$ sein, und das Produkt beider Wurzeln ist

$$\equiv -m^2 \equiv -a \pmod{p^2}.$$

Nach Ausscheidung von m und $p^2 - m$ bleiben noch $\varphi(p^2) - 2$ Zahlen, die prim zu p^2 und $< p^2$ sind. Diese lassen sich in Gruppen von je zweien so zusammenstellen, daß das Produkt der Zahlen jedes Paares

$$\equiv a \pmod{p^2}$$

sei. Da

$$\frac{1}{2} \varphi(p^2) - 1$$

solche Paare vorhanden sind, so erhalten wir als Rest des Produkts derselben

$$a^{\frac{1}{2} \varphi(p^2) - 1}.$$

Somit ist das Produkt aller Zahlen, die prim zu p^2 und $< p^2$ sind, im vorliegenden Falle, d. i. wenn a ein Rest von p^2 ist,

$$\equiv -a \cdot a^{\frac{1}{2} \varphi(p^2) - 1} \equiv -a^{\frac{1}{2} \varphi(p^2)}.$$

Wenn dagegen a ein Nichtrest von p^2 ist, so bilden die Zahlen, die prim zu p^2 und $< p^2$ sind, $\frac{1}{2} \varphi(p^2)$ Gruppen von je zwei Zahlen, deren Produkt a ist. In diesem Falle erhalten wir also für das Produkt aller dieser Zahlen den Rest

$$a^{\frac{1}{2} \varphi(p^2)} \pmod{p^2}.$$

Nun ist nach §. 108 das Produkt aller Zahlen, die prim zu p^2 und $< p^2$ sind,

$$\equiv -1 \pmod{p^2}.$$

Es ist also, wenn a ein Nichtrest von p^2 ist,

$$a^{\frac{1}{2} \varphi(p^2)} \equiv -1 \pmod{p^2},$$

dagegen, wenn a ein Rest von p^2 ist,

$$-a^{\frac{1}{2} \varphi(p^2)} \equiv -1,$$

also

$$a^{\frac{1}{2} \varphi(p^2)} \equiv +1 \pmod{p^2}.$$

Aufgaben. I. Die im vorhergehenden Beweise benutzte Gruppierung der Zahlen, die prim zu p^2 und $< p^2$ sind, für den Modul 27 vorzunehmen.

1) Es ist 19 ein Rest von 27, und man erhält

$$10 \cdot 17 \equiv -19$$

und außerdem

$$\begin{aligned} 1 \cdot 19 &\equiv 2 \cdot 23 \equiv 4 \cdot 25 \equiv 5 \cdot 20 \equiv 7 \cdot 22 \equiv 8 \cdot 26 \equiv 11 \cdot 14 \\ &\equiv 13 \cdot 16 \equiv 19 \pmod{27}, \end{aligned}$$

also ist das Gesamtprodukt

$$\equiv -19^9 \pmod{27}.$$

2) Die Zahl 2 ist ein Nichtrest von 27, und man erhält

$$\begin{aligned} 1 \cdot 2 &\equiv 4 \cdot 14 \equiv 5 \cdot 22 \equiv 7 \cdot 8 \equiv 10 \cdot 11 \equiv 13 \cdot 23 \equiv 16 \cdot 17 \\ &\equiv 19 \cdot 20 \equiv 25 \cdot 26 \equiv 2 \pmod{27}, \end{aligned}$$

also ist das Gesamtprodukt

$$\equiv 2^9 \pmod{27}.$$

II. Zu bestimmen, ob 11 Rest oder Nichtrest von 25 ist. Da

$$\varphi(25) = 20, \quad \frac{1}{2} \varphi(25) = 10$$

ist, so haben wir den Rest von $11^{10} \pmod{25}$ zu berechnen. Als solcher ergibt sich $+1$, folglich ist 11 Rest von 25.

Leichter hätte man folgendermaßen geschlossen: Da

$$11 + 25 = 36 = 6^2$$

¹⁾ Euler giebt l. c. den Satz nur für den Fall, daß der Modul eine ungerade Primzahl ist; bei dieser für praktische Anwendungen statthafter Beschränkung gestaltet sich der Beweis natürlich etwas einfacher.

ist, so ist die Kongruenz

$$x^2 \equiv 11 \pmod{25}$$

möglich und hat die Wurzeln ± 6 .

Noch einfacher wäre folgender Schluss gewesen: Da

$$11 \equiv +1 \pmod{5}$$

Rest von 5 ist, so ist die Zahl 11 auch Rest jeder Potenz von 5, also auch Rest von 25.

Anmerkung. Mag a Rest oder Nichtrest von p^2 sein, in jedem Falle erhält man durch Quadrierung des oben hergeleiteten Resultats

$$a^{\varphi(p^2)} \equiv 1 \pmod{p^2}.$$

Das ist der Ausdruck des verallgemeinerten Fermatschen Satzes für den Modul $m = p^2$.

Das Legendresche Symbol (Legendre, *Théorie des Nombres*, I, p. 197). — Wir drücken in Zukunft den Rest von $a^{\frac{1}{2}\varphi(p^2)}$ für den Modul p^2 durch das Symbol $\left(\frac{a}{p^2}\right)$ aus. Dasselbe hat also den Wert $+1$ oder -1 , jenachdem a Rest oder Nichtrest von p^2 ist.

§. 110.

Quadratischer Charakter¹⁾ eines Produkts.

Lehrsatz. Das Produkt zweier quadratischen Reste von p^2 ist ein Rest, das Produkt eines Restes in einen Nichtrest ist ein Nichtrest, das Produkt zweier Nichtreste endlich ist ein Rest.

1. Beweis (Gauss, *Disquisitiones* 98). I. Es seien a, b Reste von p^2 , die aus den Quadraten α^2, β^2 herrühren, also

$$a \equiv \alpha^2, \quad b \equiv \beta^2;$$

dann ist

$$ab \equiv (\alpha\beta)^2 \pmod{p^2},$$

d. h. ab ein Rest p^2 .

¹⁾ Man nennt die Eigenschaft einer Zahl, Rest oder Nichtrest zu sein, ihren Charakter.

II. Wenn a ein Rest, etwa $a \equiv \alpha^2$, aber b ein Nichtrest ist, so ist ab ein Nichtrest von p^2 . Wäre nämlich

$$ab \equiv k^2 \pmod{p^2},$$

so könnten wir durch Auflösung der nach §. 34 möglichen Kongruenz

$$\alpha x \equiv k \pmod{p^2}$$

einen Wert ξ von x bestimmen, für welchen $\alpha^2 \xi^2 \equiv k^2$ oder, da $\alpha^2 \equiv a$ und $k^2 \equiv ab$ sein soll, $a \xi^2 \equiv ab$ wäre. Hieraus würde aber

$$b \equiv \xi^2 \pmod{p^2}$$

folgen. Somit wäre b ein Rest von p^2 , und das ist gegen die Voraussetzung.

Oder auch: Wenn man die $\frac{1}{2} \varphi(p^2)$ Reste, die sich unter den $\varphi(p^2)$ Zahlen vorfinden, welche prim zu p^2 und $< p^2$ sind, mit a multipliziert, so erhält man $\frac{1}{2} \varphi(p^2)$ inkongruente Produkte, und jedes derselben ist ein Rest von p^2 ; auf diese Weise werden $\frac{1}{2} \varphi(p^2)$ Reste von p^2 gebildet. Wird jetzt der Nichtrest b ebenfalls mit a multipliziert, so ist das Produkt keinem der vorher erhaltenen Produkte kongruent. Wäre nun ab ebenfalls ein Rest von p^2 , so würde die Anzahl der Reste

$$\frac{1}{2} \varphi(p^2) + 1$$

betragen, und das widerspricht dem Lehrsatz I des §. 107.

III. Endlich seien a, b Nichtreste von p^2 . Wenn man dann sämtliche Reste, die sich unter den Zahlen vorfinden, welche prim zu p^2 und $< p^2$ sind, mit a multipliziert, so erhält man $\frac{1}{2} \varphi(p^2)$ inkongruente Nichtreste von p^2 . Das Produkt ab ist nun keinem der ersteren Produkte kongruent. Wäre dasselbe daher ein Nichtrest, so würde es

$$\frac{1}{2} \varphi(p^2) + 1$$

inkongruente Nichtreste von p^2 geben, was ebenfalls dem I. Lehrsatz des §. 107 widerspricht. ab ist somit ein Rest von p^2 .

2. Beweis. Das Produkt ab ist nach dem Eulerschen Kriterium ein Rest oder ein Nichtrest von p^2 , jenachdem

$$(ab)^{\frac{1}{2} \varphi(p^2)} \equiv +1 \text{ oder } \equiv -1 \pmod{p^2}$$

ist. Nun ist aber

$$(ab)^{\frac{1}{2} \varphi(p^2)} = a^{\frac{1}{2} \varphi(p^2)} \cdot b^{\frac{1}{2} \varphi(p^2)},$$

und dies Produkt hat, was den Rest für den Modul p^2 betrifft, den Wert $+1$, wenn jeder seiner beiden Faktoren entweder

$$+1 \text{ oder } -1$$

ist. Dagegen hat das Produkt den Wert -1 , wenn der eine Faktor $+1$, der andere -1 ist.

Zusatz. Ein Produkt beliebig vieler Faktoren ist Rest oder Nichtrest von p^2 , jenachdem es eine gerade oder eine ungerade Anzahl von Faktoren enthält, die Nichtreste von p^2 sind.

Bei Anwendung des Legendreschen Symbols wird dieser Zusatz durch die Formel

$$\left(\frac{ab \dots c}{p^2}\right) = \left(\frac{a}{p^2}\right) \left(\frac{b}{p^2}\right) \dots \left(\frac{c}{p^2}\right)$$

ausgedrückt.

Beispiel. Die Zahl 27 hat nach §. 107 die Reste

$$(1) \quad 1, 4, 7, 10, 13, 16, 19, 22, 25,$$

die Nichtreste

$$(2) \quad 2, 5, 8, 11, 14, 17, 20, 23, 26,$$

und man überzeugt sich leicht, daß der Rest des Produkts sowohl zweier Zahlen von (1) als auch zweier Zahlen von (2) eine Zahl von (1) ist, während die Multiplikation einer Zahl von (1) mit einer Zahl von (2) eine Zahl von (2) liefert.

Anmerkung. Es ist eine empfehlenswerte Übung, den vorhergehenden Satz und einige der früheren Sätze durch Anwendung der Indizes zu beweisen. Man erkennt leicht, daß der Index einer Zahl a , gleichgültig welche primitive Wurzel man als Basis genommen hat, gerade oder ungerade ist, jenachdem a quadratischer Rest oder Nichtrest des Moduls ist.

§. 111.

Reste der Potenzen von 2.

Da wir nur die Zahlen betrachten, welche prim zum Modul sind, und da kongruente Zahlen von demselben quadratischen Charakter sind, so handelt es sich hier nur um die ungeraden Zahlen, welche kleiner als der Modul sind, also für den Modul 2 nur um die Zahl 1, für den Modul 4 um die Zahlen 1 und 3, für den Modul 8 um 1, 3, 5 und 7, u. s. w.

Der Modul sei erstens 2. Die Kongruenz

$$x^2 \equiv 1 \pmod{2}$$

hat die eine Wurzel

$$x \equiv +1 \equiv -1 \pmod{2}.$$

Die Zahl 1 ist also Rest von 2, Nichtreste giebt es für diesen Modul nicht.

Der Modul sei zweitens 4. Da x^2 bei der Division durch 4 einen ungeraden Rest (1 oder 3) geben soll, so muß x selbst ungerade sein, etwa

$$x = 2n + 1.$$

Dann ist

$$x^2 = 4n^2 + 4n + 1 \equiv 1 \pmod{4}.$$

Daraus ersehen wir, daß 1 Rest, 3 Nichtrest von 4 ist, d. h. daß die Kongruenz

$$x^2 \equiv 1 \pmod{4}$$

möglich, die Kongruenz

$$x^2 \equiv 3 \pmod{4}$$

unmöglich ist. Die Kongruenz

$$x^2 \equiv 1 \pmod{4}$$

hat zwei Wurzeln, nämlich 1 und 3 oder ± 1 .

Drittens sei der Modul 8. Es ist

$$(4n \pm 1)^2 = 16n^2 \pm 8n + 1 \equiv 1 \pmod{8},$$

also das Quadrat jeder ungeraden Zahl von der Form $8k \pm 1$. Danach ist 1 Rest von 8, während 3, 5, 7 Nichtreste sind. Die Kongruenz

$$x^2 \equiv 1 \pmod{8}$$

ist also möglich; sie hat die vier Wurzeln 1, 3, 5, 7 oder ± 1 , ± 3 . Die Kongruenzen $x^2 \equiv 3$ oder 5 oder 7 (mod. 8) sind unmöglich.

Endlich sei der Modul 2^κ , wo $\kappa > 3$ vorausgesetzt wird. Wenn

$$x^2 \equiv a \pmod{2^\kappa, \kappa > 3}$$

ist, so muß auch

$$x^2 \equiv a \pmod{8}$$

sein, da eine durch 2^κ , $\kappa > 3$ teilbare Zahl $x^2 - a$ jedenfalls auch durch 8 teilbar ist. Die Kongruenz

$$x^2 \equiv a \pmod{8}$$

erfordert aber, daß a die Form $8n + 1$ habe, sie ist unmöglich für $a = 8n + 3, 5, 7$. Für diese drei Formen ist also auch die Kongruenz

$$x^2 \equiv a \pmod{2^\kappa, \kappa > 3}$$

unmöglich. Wir wollen nun zeigen, daß sie für jedes a , welches die Form $8n + 1$ hat, möglich ist und dann vier inkongruente Wurzeln besitzt. Zu diesem Zwecke zeigen wir, daß und wie aus jeder Wurzel einer Kongruenz

$$(1) \quad x^2 \equiv a \pmod{2^\nu, \nu \leq 3}$$

eine und nur eine Wurzel der Kongruenz

$$(2) \quad x^2 \equiv a \pmod{2^{\nu+1}}$$

hergeleitet werden kann.

Es sei also α eine Wurzel von (1). Da a ungerade ist, so muß auch α eine ungerade Zahl sein, ebenso die gesuchte Wurzel von (2). Wir nehmen daher

$$x = \alpha + 2^{\nu-1}y$$

an und suchen über y so zu verfügen, daß der angegebene Wert von x dann der Kongruenz (2) genüge. Wird derselbe quadriert, so erhält man

$$x^2 = \alpha^2 + 2^\nu \alpha y + 2^{2\nu-2}y^2.$$

Nun ist

$$2\nu - 2 = (\nu + 1) + (\nu - 3),$$

also, wenn $\nu = 3$ ist,

$$2\nu - 2 = \nu + 1,$$

für $\nu > 3$ aber

$$2\nu - 2 > \nu + 1.$$

Daher ist im vorliegenden Falle

$$2^{2^r-2} \equiv 0 \pmod{2^{r+1}},$$

und wir erhalten durch Einsetzung des für x^2 hergeleiteten Wertes in (2)

$$(3) \quad \alpha^2 + 2^r \alpha y \equiv a \pmod{2^{r+1}}.$$

Da aber α eine Wurzel von (1) ist, so ist $a - \alpha^2$ ein Vielfaches von 2^r , etwa $= \beta \cdot 2^r$. Die Kongruenz (3) geht also, wenn α^2 auf die rechte Seite gebracht und dann beiderseits durch 2^r dividiert wird, über in

$$\alpha y \equiv \beta \pmod{2}$$

oder, da α als ungerade Zahl $\equiv 1 \pmod{2}$ ist, in

$$(4) \quad y \equiv \beta \pmod{2}.$$

Diese Kongruenz, welche die Wurzel 0 oder 1 hat, jenachdem β gerade oder ungerade ist, bestimmt y , und durch Einsetzung des Wertes von y in den Ausdruck

$$x = \alpha + 2^{r-1}y$$

erhalten wir die Wurzel von (2), welche der Wurzel α von (1) entspricht. Die Kongruenz (2) hat also ebenso viele Wurzeln, wie (1), und mit Bezugnahme auf das für den Modul 8 gefundene Resultat ergibt sich der Satz:

Für den Modul 2^x , $x \geq 3$ sind die Zahlen $8n + 1$ Reste die Zahlen $8n + 3, 5, 7$ Nichtreste, und die Kongruenz

$$x^2 \equiv a \pmod{2^x}$$

hat, wenn a ein Rest ist, vier inkongruente Wurzeln.

Von den 2^{x-1} ungeraden Zahlen, die $< 2^x$ sind, hat $\frac{1}{4}$ die Form $8n + 1$. Der Modul 2^x , $x \geq 3$, hat also

$$\frac{1}{4} \cdot 2^{x-1} = 2^{x-3}$$

Reste und $3 \cdot 2^{x-3}$ Nichtreste.

Anmerkung. Wenn α das eine Wurzelpaar der Kongruenz

$$x^2 \equiv a \pmod{2^x, x \geq 3}$$

ist, so ist

$$+ (2^{x-1} - \alpha)$$

das zweite Paar.

Es ist nämlich .

$$[\pm (2^{x-1} - \alpha)]^2 = 2^{2x-2} - 2^x \alpha + \alpha^2 \equiv \alpha^2 \pmod{2^x}.$$

Wenn also α eine Wurzel der vorgelegten Kongruenz ist, so wird dieselbe auch durch $2^{x-1} - \alpha$ befriedigt, und beide Zahlen können, sobald $x \geq 3$ ist, nicht kongruent sein; denn wenn

$$\alpha \equiv 2^{x-1} - \alpha \pmod{2^x}$$

wäre, so müßte $2\alpha \equiv 2^{x-1}$, also $\alpha \equiv 2^{x-2}$ sein; α wäre daher eine gerade Zahl, was unmöglich ist.

Beispiel. Die Kongruenz $x^2 \equiv 17$ hat für den

Modul 8	die Wurzeln	+ 1,	+ 3,
" 16	"	+ 1,	+ 7,
" 32	"	+ 7,	+ 9,
" 64	"	+ 9,	+ 23.

§. 112.

Die rein quadratische Kongruenz für einen beliebig zusammengesetzten Modul.

Wir betrachten jetzt die Kongruenz

$$(1) \quad x^2 \equiv a \pmod{2^x p^\lambda q^\mu \dots},$$

wo $x, \lambda, \mu, \dots$ ganze positive Zahlen und $p, q, \dots$ voneinander verschiedene ungerade Primzahlen bezeichnen, deren Anzahl n sein möge. Wenn die Kongruenz (1) möglich ist, etwa durch den Wert $x = \xi$ befriedigt wird, so ist $\xi^2 - a$ durch jede der Zahlen $2^x, p^\lambda, q^\mu, \dots$ teilbar, d. h. ξ ist eine Wurzel jeder der Kongruenzen

$$(2) \quad \begin{cases} x^2 \equiv a \pmod{2^x} \\ x^2 \equiv a \pmod{p^\lambda} \\ x^2 \equiv a \pmod{q^\mu} \\ \dots \end{cases}$$

mit anderen Worten: Wenn die Zahl a ein Rest des Moduls $2^x p^\lambda q^\mu \dots$ ist, so ist sie auch Rest jedes der Faktoren

$$2^x, p^\lambda, q^\mu, \dots$$

Wenn a für einen einzigen dieser Faktoren Nichtrest ist, so ist sie auch Nichtrest für das Produkt derselben.

Wenn umgekehrt die Kongruenzen (2) möglich sind, so ist auch (1) möglich, d. h. a ein Rest von $2^x p^2 q^u \dots$

Es sei nämlich

$$a \equiv \alpha^2 \pmod{2^x}, \quad a \equiv \beta^2 \pmod{p^2}, \quad \dots$$

Wird dann eine Zahl ξ bestimmt, welche den Bedingungen

$$\xi \equiv \alpha \pmod{2^x}, \quad \xi \equiv \beta \pmod{p^2}, \quad \dots$$

genügt, so ist

$$\xi^2 \equiv \alpha^2 \equiv a \pmod{2^x}, \quad \xi^2 \equiv \beta^2 \equiv a \pmod{p^2}, \quad \dots,$$

folglich ist $\xi^2 - a$ durch jede der Zahlen

$$2^x, \quad p^2, \quad q^u, \quad \dots$$

teilbar, und da diese letzteren prim zu einander sind, so geht auch ihr Produkt in $\xi^2 - a$ auf, d. h. ξ ist eine Wurzel der Kongruenz (1).

Anzahl der Wurzeln der Kongruenz (1). — Um alle Wurzeln von (1) zu erhalten, haben wir jede Wurzel einer der Kongruenzen (2) mit jeder Wurzel jeder der anderen Kongruenzen (2) zu kombinieren. Nun sind — bei vorläufigem Ausschluss der ersten der Kongruenzen (2) — n Kongruenzen (2) vorhanden, von denen jede zwei Wurzeln besitzt. Diese gestatten 2^n Kombinationen. Da nun die erste der Kongruenzen (2), wie wir oben gesehen haben, eine oder zwei oder vier Wurzeln besitzt, jenachdem ihr Modul $= 2, = 4$ oder $\equiv 8$ ist, so ergeben sich für die Kongruenz (1) im ganzen

$$2^n \text{ oder } 2 \cdot 2^n \text{ oder } 4 \cdot 2^n$$

Wurzeln, jenachdem $x = 1, = 2$ oder > 2 ist.

Beispiele.

$$\text{I. } x^2 \equiv 37 \pmod{84 = 2^2 \cdot 3 \cdot 7} \\ [\pm 11, \pm 17, \pm 25, \pm 31].$$

$$\text{II. } x^2 \equiv 111 \pmod{125 = 5^3} \\ [\pm 19].$$

$$\text{III. } x^2 \equiv 55 \pmod{162 = 2 \cdot 3^4} \\ [\pm 53].$$

$$\text{IV. } x^2 \equiv 319 \pmod{378 = 2 \cdot 3^3 \cdot 7} \\ [\pm 47, \pm 61].$$

$$\text{V. } x^2 \equiv 181 \pmod{330 = 2 \cdot 3 \cdot 5 \cdot 11} \\ [\pm 29, \pm 59, \pm 161, \pm 191].$$

$$\text{VI. } x^2 \equiv 49 \pmod{120 = 2^3 \cdot 3 \cdot 5} \\ [+ 7, + 13, + 17, + 23, + 37, + 43, + 47, + 53].$$

$$\text{VII. } x^2 \equiv 521 \pmod{1040 = 2^4 \cdot 5 \cdot 13} \\ [+ 51, + 131, + 181, + 259, + 261, + 339, + 389, + 469].$$

$$\text{VIII. } x^2 \equiv 25 \pmod{357 = 3 \cdot 7 \cdot 17} \\ [+ 5, + 107, + 124, + 131].$$

§. 113.

Der verallgemeinerte Wilsonsche Satz (Gauss, Disquisitiones, 78).

In §. 108 ist der Wilsonsche Satz auf den Fall ausgedehnt worden, in welchem der Modul eine Potenz einer ungeraden Primzahl ist. Die Frage, welchen Rest das Produkt aller Zahlen giebt, die prim zu einem beliebigen Modul und kleiner als dieser Modul sind, beantwortet der folgende

Lehrsatz. Das Produkt aller Zahlen, die prim zu einem Modul m und $< m$ sind, ist

$$\equiv -1 \pmod{m},$$

wenn m eine Potenz¹⁾ einer ungeraden Primzahl oder das Doppelte einer solchen Potenz oder 4 ist. In allen anderen Fällen ist das Produkt

$$\equiv +1 \pmod{m}.$$

Beweis. Unter den Zahlen, die prim zu m und $< m$ sind, befinden sich zunächst diejenigen, welche der Kongruenz

$$(1) \quad x^2 \equiv 1 \pmod{m}$$

nicht genügen. Diese lassen sich zu je zweien so zusammenstellen, daß das Produkt der beiden Zahlen jedes Paares

$$\equiv +1 \pmod{m}$$

ist. Wenn nämlich a eine dieser Zahlen ist, so hat die Kongruenz

$$(2) \quad ax \equiv 1 \pmod{m}$$

stets eine, aber auch nur eine Wurzel α , die ebenfalls prim zu m ist und $< m$ vorausgesetzt werden darf, und die von a ver-

¹⁾ Der Fall, in welchem m eine ungerade Primzahl ist, ist eingeschlossen.

schieden sein muß, da sonst a der Kongruenz (1) genügen würde. Bezeichnet weiter b eine von a und α verschiedene Zahl, die ebenfalls prim zu m und $< m$ ist und der Kongruenz (1) nicht genügt, so läßt sich auch ihr durch Lösung der Kongruenz

$$bx \equiv 1 \pmod{m}$$

eine Zahl β zuordnen, die von b verschieden, prim zu m und $< m$ sein wird. Diejenigen von den hier in Betracht kommenden Zahlen, welche der Kongruenz (1) nicht genügen, bilden also Paare von je zwei Zahlen, deren Produkt

$$\equiv +1 \pmod{m}$$

ist. Somit ist das Produkt aller dieser Zahlen gleichfalls

$$\equiv +1 \pmod{m}.$$

Wir haben jetzt noch das Produkt der Wurzeln von (1) zu bestimmen, deren Anzahl wir in §. 112 gefunden haben.

Wenn eine Zahl ξ eine Wurzel von (1), also

$$\xi^2 \equiv 1 \pmod{m}$$

ist, so genügt auch ihre Ergänzung zum Modul, d. i. $m - \xi$ dieser Kongruenz, denn es ist

$$(m - \xi)^2 \equiv \xi^2 \pmod{m}.$$

Nun ist aber das Produkt dieser beiden Wurzeln

$$\xi(m - \xi) \equiv -1 \pmod{m},$$

folglich lassen sich die Wurzeln von (1) ebenfalls zu je zweien zusammenstellen, aber in der Weise, daß das Produkt der Wurzeln für jedes Paar

$$\equiv -1 \pmod{m}$$

sei. Wenn also die Anzahl aller Wurzeln durch 4 oder durch eine höhere Potenz von 2 teilbar ist, so ist das Produkt aller Wurzeln und somit das Gesamtprodukt aller Zahlen, die prim zu m und $< m$ sind,

$$\equiv +1 \pmod{m}.$$

Wenn aber die Kongruenz (1) nur zwei Wurzeln besitzt, sich also nur ein Wurzelpaar ergibt, so ist das Produkt der Wurzeln und somit das Gesamtprodukt aller Zahlen, die prim zu m und $< m$ sind,

$$\equiv -1 \pmod{m}.$$

Die Kongruenz (1) hat aber nach §. 112 nur zwei Wurzeln:

- 1) wenn der Modul eine ungerade Primzahl oder eine Potenz einer ungeraden Primzahl ist;
- 2) wenn der Modul das Doppelte einer solchen Potenz ist;
- 3) wenn der Modul gleich 4 ist.

Damit ist der Satz vollständig bewiesen.

Beispiele. I. Die Kongruenz

$$x^2 \equiv 1 \pmod{50}$$

hat die Wurzeln 1 und 49, und es ist mod. 50

$$\begin{aligned} 1.49 &\equiv -1, & 3.17 &\equiv 7.43 \equiv 9.39 \equiv 11.41 \equiv 13.27 \\ &\equiv 19.29 \equiv 21.31 & 23.37 &\equiv 33.47 \equiv +1, \end{aligned}$$

also das Produkt aller Zahlen, die prim zu 50 und < 50 sind,
 $\equiv -1 \pmod{50}$.

II. Für den Modul 35 ist

$$1.34 \equiv -1, \quad 6.29 \equiv -1,$$

ferner

$$\begin{aligned} 2.18 &\equiv 3.12 \equiv 4.9 \equiv 8.22 \equiv 11.16 \equiv 13.27 \equiv 17.33 \\ &\equiv 19.24 \equiv 23.32 \equiv 26.31 \equiv +1, \end{aligned}$$

also das Produkt-

$$\equiv +1 \pmod{35}.$$

III. Für den Modul 24 ist

$$1.23 \equiv -1, \quad 5.19 \equiv -1, \quad 7.17 \equiv -1, \quad 11.13 \equiv -1,$$

also das Produkt

$$\equiv +1 \pmod{24}.$$

§. 114.

Für welche Moduln ist eine gegebene Zahl ein quadratischer Rest, und für welche ist sie Nichtrest?

Im Vorhergehenden haben wir untersucht, welches die inkongruenten quadratischen Reste eines gegebenen Moduls seien, oder für welche Werte von a bei gegebenem m die Kongruenz

$$x^2 \equiv a \pmod{m}$$

möglich sei, und wieviele Wurzeln sie in jedem Falle habe. Wir wenden uns jetzt zu der weit schwierigeren Frage: Für welche Moduln m ist die Kongruenz

$$x^2 \equiv a \pmod{m}$$

bei gegebenem a möglich, oder welches sind die Moduln m , für welche eine gegebene Zahl a quadratischer Rest ist?

Die Moduln m , für welche die Kongruenz $x^2 - a \equiv 0$ möglich ist, nennt man auch die Divisoren der Form $x^2 - a$, weil es Zahlen x giebt, für welche $x^2 - a$ durch m teilbar ist. Die Divisoren von $x^2 - a$ stimmen überein mit denjenigen der Form $t^2 - au^2$, in welcher t, u zwei unbestimmte ganze Zahlen sein sollen, die wir immer als prim zu einander voraussetzen. Dafs ein Divisor von $x^2 - a$ auch ein Divisor von $t^2 - au^2$ ist, geht daraus hervor, dafs die letztere Form in die erstere übergeht, wenn

$$t = x, \quad u = 1$$

angenommen wird. Ist umgekehrt m ein Divisor von $t^2 - au^2$, so läfst sich zeigen, dafs sich ein Wert von x bestimmen läfst, für welchen $x^2 - a$ durch m teilbar wird. Wenn nämlich m in $t^2 - au^2$ aufgeht, so mufs m prim zu u sein; denn ein gemeinschaftlicher Divisor beider Zahlen müfste auch in t^2 , somit auch in t aufgehen, während t, u als prim zu einander vorausgesetzt werden. Folglich ist die Kongruenz

$$ux \equiv t \pmod{m}$$

möglich und hat eine einzige Wurzel

$$x \equiv \xi \pmod{m}.$$

Es ist also

$$u^2 \xi^2 \equiv t^2 \pmod{m},$$

und somit geht die Kongruenz

$$t^2 - au^2 \equiv 0$$

über in

$$u^2 \xi^2 - au^2 \equiv 0$$

oder

$$\xi^2 - a \equiv 0 \pmod{m},$$

d. h. wenn die Zahl m ein Divisor von $t^2 - au^2$ ist, so ist sie auch ein Divisor von $x^2 - a$.

Bei der Aufsuchung der Moduln, für welche eine gegebene Zahl a Rest ist, werden wir uns auf die Moduln beschränken,

welche prim zu a sind, und da nach §. 112 die Möglichkeit der Kongruenz

$$x^2 \equiv a \pmod{m}$$

von der Beschaffenheit der in m enthaltenen Primzahlen abhängt und die Potenzen von 2 in §. 111 ihre Erledigung gefunden haben, so haben wir nur die ungeraden Primzahlen zu ermitteln, für welche a quadratischer Rest ist. Eine weitere Vereinfachung erfährt die Aufgabe noch durch den §. 110, welcher den quadratischen Charakter eines Produkts aus dem seiner Faktoren bestimmen lehrt. Da nun eine Zahl positiv oder negativ, gerade oder ungerade sein kann, so kommt es im Grunde nur auf die Beantwortung folgender Fragen an:

- 1) Von welchen ungeraden Primzahlen p ist -1 quadratischer Rest und von welchen Nichtrest?
- 2) Von welchen ist es die Zahl 2?
- 3) Von welchen ist es eine andere ungerade Primzahl q ?

§. 115.

Moduln, für welche -1 quadratischer Rest ist.

(Euler, Opuscula analytica I, p. 121 = Commentationes arithmet. collectae I, p. 487.)

Lehrsatz. Die Zahl -1 ist Rest aller Primzahlen p der Form $4n + 1$, Nichtrest aller Primzahlen p der Form $4n + 3$, oder es ist

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}.$$

1. Beweis. Nach dem Eulerschen Kriterium (§. 109) ist -1 Rest aller Primzahlen p , für welche

$$(-1)^{\frac{1}{2}(p-1)} = +1,$$

also

$$\frac{1}{2}(p-1)$$

eine gerade Zahl ist. Wird

$$\frac{1}{2}(p-1) = 2n$$

gesetzt, so ergibt sich

$$p = 4n + 1.$$

Dagegen ist -1 Nichtrest aller Primzahlen p , für welche

$$(-1)^{\frac{1}{2}(p-1)} = -1, \text{ also } \frac{1}{2}(p-1)$$

eine ungerade Zahl ist. Wird

$$\frac{1}{2}(p-1) = 2n + 1$$

gesetzt, so ergibt sich

$$p = 4n + 3.$$

Jenachdem umgekehrt

$$p = 4n + 1$$

oder

$$= 4n + 3$$

ist, erhalten wir

$$\frac{1}{2}(p-1) = 2n \text{ oder } = 2n + 1,$$

also

$$(-1)^{\frac{1}{2}(p-1)} = +1 \text{ oder } = -1.$$

2. Beweis. Unter den Zahlen

$$1, 2, 3, \dots, p-1$$

befinden sich nach §. 106 $\frac{p-1}{2}$ quadratische Reste und ebenso viele Nichtreste von p . Die Anzahl der Nichtreste ist also gerade, wenn p die Form $4n+1$ hat, ungerade dagegen für $p = 4n+3$. Im ersten Falle ist somit nach §. 110 das Produkt aller Zahlen

$$1, 2, 3, \dots, p-1$$

ein Rest, im zweiten ein Nichtrest. Dieses Produkt ist aber nach dem Wilsonschen Satze immer

$$\equiv -1 \pmod{p};$$

daher wird auch -1 im ersten Falle ein Rest, im zweiten ein Nichtrest sein.

Zusatz I. Jede Primzahl der Form $4n + 1$ kann als Summe zweier Quadrate dargestellt werden, welche prim zu einander sind. (Fermat, Bemerkung zu Diophant III, 22 = Oeuvres I, p. 294. Siehe auch II, p. 403. Euler, Commentationes arithmet. collectae I, p. 155.)

Beweis. Wenn

$$p = 4n + 1$$

ist, so ist -1 ein quadratischer Rest von p , d. h. es läßt sich eine Zahl a bestimmen, für welche

$$a^2 \equiv -1 \pmod{p},$$

also $a^2 + 1$ durch p teilbar ist. Daher muß nach §. 61, Lehrsatz II, p selbst die Summe zweier Quadrate sein. Diese beiden Quadrate können aber keinen gemeinschaftlichen Divisor haben, weil ein solcher auch in p aufgehen müßte.

Auf welche Weise

$$p = 4n + 1$$

in zwei Quadrate zerfällt wird, ist in §. 61, Aufgabe III gezeigt worden.

Aufgabe. Die Primzahl 1997 in zwei Quadrate zu zerfallen.

Lösung. Da 2 eine primitive Wurzel von 1997 ist, so ist

$$2^{998} \equiv -1 \text{ oder } (2^{499})^2 \equiv -1,$$

also 2^{499} eine Wurzel der Kongruenz

$$x^2 \equiv -1 \pmod{1997}.$$

Nun findet man (bei Anwendung einer Tabelle der Quadratzahlen) leicht, daß mod. 1997

$$2^{10} \equiv 1024, \quad 2^{20} \equiv 151, \quad 2^{40} \equiv 834, \quad 2^{80} \equiv 600, \quad 2^{160} \equiv 540, \\ 2^{320} \equiv 38, \quad 2^{480} \equiv 550, \quad 2^{499} \equiv -412$$

ist. Somit sind die Wurzeln unserer Kongruenz ± 412 . Weiter ergibt sich

$$\frac{1997}{412} = (4, 1, 5, 1, 1, 5, 1, 4),$$

4	1	5	1	
1	4	5	29	34,

folglich

$$1997 = 29^2 + 34^2.$$

Zusatz II. Die Zahlen a und $p - a$ sind mod. p von demselben oder von entgegengesetztem quadratischem Charakter, jenachdem die Primzahl p die Form $4n + 1$ oder $4n + 3$ hat.

§. 116.

Moduln, für welche $+ 2$ quadratischer Rest ist.

Um zu bestimmen, für welche Primzahlen p als Moduln die Kongruenz $x^2 \equiv 2$ möglich sei, können wir beiderseits die Indizes für eine beliebige Basis g nehmen. Wir erhalten

$$2 \text{ Ind. } x \equiv \text{Ind. } 2 \pmod{p-1}.$$

Da nun der Koeffizient von Ind. x und der Modul $p - 1$ den größten gemeinschaftlichen Divisor 2 haben, so ist die letzte Kongruenz und somit auch die Kongruenz

$$x^2 \equiv 2 \pmod{p}$$

nur möglich, wenn Ind. 2 eine gerade Zahl ist. Die Zahl 2 ist also ein quadratischer Rest aller Primzahlen p , für welche Ind. 2 gerade ist. Nach den Indizestafeln sind dies die Zahlen

$$p = 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97,$$

also alle unter 100 liegenden Primzahlen der beiden Formen

$$8n + 1, \quad 8n + 7.$$

Dagegen ist nach den Indizestafeln Ind. 2 ungerade, also 2 ein Nichtrest der Primzahlen

$$p = 3, 5, 11, 13, 19, 29, 37, 43, 53, 59, 61, 67, 83,$$

das ist aller unter 100 liegenden Primzahlen der beiden Formen

$$8n + 3, \quad 8n + 5.$$

Nun ist für

$p =$	$8n + 1$	$8n + 3$	$8n + 5$	$8n + 7$
$\frac{p-1}{2} =$	$4n$	$4n + 1$	$4n + 2$	$4n + 3$
$\frac{p+1}{2} =$	$4n + 1$	$4n + 2$	$4n + 3$	$4n + 4$
$\frac{p^2-1}{4} =$	$4n(4n+1)$	$(4n+1)(4n+2)$	$(4n+2)(4n+3)$	$(4n+3)(4n+4)$
$\frac{p^2-1}{8} =$	$2n(4n+1)$	$(4n+1)(2n+1)$	$(2n+1)(4n+3)$	$(4n+3)(2n+2)$

und da

$$2n(4n+1) \quad \text{und} \quad (4n+3)(2n+2)$$

gerade, dagegen

$$(4n+1)(2n+1) \quad \text{und} \quad (2n+1)(4n+3)$$

ungerade Zahlen sind, so gilt für die Primzahlen unter 100 die Formel

$$\left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)}.$$

Wir beweisen jetzt, daß es sich allgemein so verhält, also den von Fermat (Varia Opera, p. 168 = Oeuvres II, p. 231 und Oeuvres II, p. 403) entdeckten und von Lagrange (Oeuvres III, p. 775) zuerst bewiesenen

Lehrsatz. Die Zahl 2 ist ein quadratischer Rest aller Primzahlen der Formen

$$8n + 1, \quad 8n + 7,$$

Nichtrest dagegen aller Primzahlen der Formen

$$8n + 3, \quad 8n + 5.$$

Beweis. Es sei zunächst $p = 8n + 1$. Wenn dann m eine beliebige durch p nicht teilbare Zahl bezeichnet, so ist nach dem Fermatschen Satze

$$m^{8n} = (m^{4n})^2 \equiv 1,$$

also

$$m^{4n} \equiv +1 \quad \text{oder} \quad \equiv -1 \pmod{p}.$$

Wird nun m durch eine primitive Wurzel g ersetzt, so kann g^{4n} nicht

$$\equiv +1 \pmod{p}$$

sein, da sonst g der Voraussetzung zuwider schon zum Exponenten

$$4n = \frac{1}{2}(p-1)$$

gehören würde. Es ist also

$$g^{4n} \equiv -1 \quad \text{oder} \quad g^{4n} + 1 \equiv 0 \pmod{p}.$$

Nun ergibt sich aber

$$(g^{2n} + 1)^2 = g^{4n} + 2g^{2n} + 1,$$

also wegen der letzten Kongruenz

$$(g^{2n} + 1)^2 \equiv 2g^{2n} \pmod{p}.$$

Danach ist $2g^{2n}$ ein quadratischer Rest von p , und da g^{2n} ein durch p nicht teilbares Quadrat ist, so muß 2 ein Rest sein. Die Zahl 2 ist also Rest jeder Primzahl der Form $8n + 1$.

Zweitens nehmen wir an, es sei

$$p = 8n + 3 \quad \text{oder} \quad 8n + 5.$$

Wenn es Primzahlen dieser Formen gäbe, für welche 2 ein quadratischer Rest wäre, so müßte eine derselben die kleinste sein. Diese soll mit t bezeichnet werden. Dann ist also t eine Primzahl einer der beiden Formen

$$8n + 3, \quad 8n + 5,$$

für welche die Kongruenz $x^2 \equiv 2$ möglich ist. Diese Kongruenz hat nach §. 106 zwei Wurzeln ξ und $-\xi \equiv t - \xi$, von denen jede $< t$ ist. Wenn die eine dieser Wurzeln ungerade ist, so wird die andere gerade sein; denn ihre Summe ist ungerade, nämlich $= t$. Wir dürfen daher voraussetzen, ξ sei ungerade und $< t$. Nun soll

$$\xi^2 \equiv 2 \pmod{t}$$

oder

$$\xi^2 = 2 + tu, \quad tu = \xi^2 - 2$$

sein, wo u eine ganze Zahl bezeichnet. Dann ist $tu < \xi^2$. Aus $\xi < t$ folgt aber $\xi^2 < t^2$, also ist um so mehr $tu < t^2$ oder $u < t$. Weiter hat ξ^2 als Quadrat einer ungeraden Zahl die Form $8n + 1$, also $tu = \xi^2 - 2$ die Form $8n - 1$, und daher muß u die Form $8n + 5$ oder $8n + 3$ haben, je nachdem t von der Form $8n + 3$ oder $8n + 5$ ist.

Aus der Gleichung $\xi^2 = 2 + tu$ folgt aber, daß auch

$$\xi^2 \equiv 2 \pmod{u}$$

ist. Die Kongruenz $x^2 \equiv 2$ besteht also auch für einen Modul u , der $< t$ und ebenfalls von einer der beiden Formen $8n + 3$, $8n + 5$ ist.

Dies widerspricht, wenn u eine Primzahl ist, der Voraussetzung, nach welcher t die kleinste Primzahl dieser beiden Formen sein soll, für welche 2 quadratischer Rest ist. Ist dagegen u eine zusammengesetzte Zahl, so muß diese wenigstens einen Primfaktor v einer der beiden Formen

$$8n + 3, \quad 8n + 5$$

enthalten; denn Faktoren der Formen

$$8n + 1, \quad 8n + 7$$

können niemals ein Produkt der Form $8n + 3$ oder $8n + 5$ geben. Da dann 2 auch Rest von v sein müßte und v ebenfalls $< t$ ist, so würde sich derselbe Widerspruch ergeben. Die Zahl 2 ist also Nichtrest aller Primzahlen der Formen

$$8n + 3, \quad 8n + 5.$$

Endlich ist noch zu beweisen, daß 2 Rest der Primzahlen $8n + 7$ ist. Da nach §. 115 die Zahl -1 Nichtrest dieser Primzahlen ist, so haben wir nur darzuthun, daß -2 Nichtrest der Primzahlen $8n + 7$ ist. Statt dessen beweisen wir, daß -2 Nichtrest aller Primzahlen der beiden Formen

$$8n + 5, \quad 8n + 7$$

ist.

Die Zahl 5 hat die Nichtreste 2 und $3 \equiv -2$, die Zahl 7 die Nichtreste 3, 6 und $5 \equiv -2$. Für die Moduln 5 und 7 ist also -2 jedenfalls Nichtrest. Wenn nun unsere Behauptung nicht allgemein richtig ist, d. h. wenn es Primzahlen der Formen

$$8n + 5, \quad 8n + 7$$

gibt, für welche -2 Rest ist, so muß eine derselben die kleinste sein. Wird dieselbe mit t bezeichnet und die ungerade Wurzel der Kongruenz

$$x^2 \equiv -2 \pmod{t}$$

§ genannt, so erhalten wir

$$\xi^2 \equiv -2 \pmod{t}, \quad \xi^2 = -2 + tu, \quad \xi^2 + 2 = tu,$$

und hieraus folgt, da $\xi < t$ ist, $u < t$.

Weiter muß u , wie sich leicht zeigen läßt, von der Form

$$8n + 5 \quad \text{oder} \quad 8n + 7$$

sein, jenachdem t die Form

$$8n + 7 \quad \text{oder} \quad 8n + 5$$

hat. Endlich folgt aus der Annahme

$$-2 = \xi^2 - tu$$

noch

$$\xi^2 \equiv -2 \pmod{u},$$

also muß -2 auch Rest von u sein. Das widerspricht, wenn u eine Primzahl ist, der Voraussetzung, nach welcher t die kleinste Primzahl der Formen

$$8n + 5, \quad 8n + 7$$

sein soll, für welche -2 Rest ist. Wenn aber u eine zusammengesetzte Zahl ist, so muß diese wenigstens einen Primfaktor $v < u$ einer der Formen

$$8n + 5, \quad 8n + 7$$

haben, und für v muß dann -2 ebenfalls Rest sein. Das widerspricht aber auch der Voraussetzung. Die Zahl -2 ist also Nichtrest aller Primzahlen

$$8n + 5, \quad 8n + 7,$$

und somit ist 2 Rest aller Primzahlen $8n + 7$.

Zusatz. Die Zahl -2 ist Rest aller Primzahlen

$$8n + 1, \quad 8n + 3,$$

Nichtrest aller Primzahlen

$$8n + 5, \quad 8n + 7.$$

Beweis. Der zweite Teil des Satzes ist oben bewiesen. Was den ersten Teil betrifft, so ist für $p = 8n + 1$

$$\left(\frac{-1}{p}\right) = +1, \quad \left(\frac{2}{p}\right) = +1,$$

also

$$\left(\frac{-2}{p}\right) = +1,$$

und für $p = 8n + 3$

$$\left(\frac{-1}{p}\right) = -1, \quad \left(\frac{2}{p}\right) = -1,$$

also

$$\left(\frac{-2}{p}\right) = +1.$$

§. 117.

Gauss' Kriterium zu entscheiden, ob eine gegebene Zahl Rest oder Nichtrest einer ungeraden Primzahl sei (Werke Bd. II, S. 51).

Lehrsatz. Es sei p eine positive ungerade Primzahl, M eine durch p nicht teilbare ganze Zahl. Man nehme die kleinsten positiven Reste der Produkte

$$M, 2M, 3M, \dots, \frac{1}{2}(p-1)M$$

für den Modul p . Diese Reste werden teils kleiner, teils gröfser als $\frac{1}{2}p$ sein. Die Anzahl der letzteren sei n . Dann ist M ein quadratischer Rest oder Nichtrest von p , jenachdem n gerade oder ungerade ist.

Beweis. Es seien $a, b, c, d, \dots$ diejenigen dieser Reste, welche kleiner als $\frac{1}{2}p$ sind; die übrigen, die gröfser als $\frac{1}{2}p$ sind, seien $a', b', c', d', \dots$. Dann werden die Ergänzungen der letzteren zum Modul p , nämlich

$$p - a', p - b', p - c', p - d', \dots$$

sämtlich kleiner als $\frac{1}{2}p$ und sowohl untereinander als auch von den Resten $a, b, c, d, \dots$ verschieden sein. Denn wenn

$$p - a' \equiv p - b' \pmod{p}$$

wäre, so müfste $a' \equiv b' \pmod{p}$ sein; es wären also zwei der oben angegebenen Produkte und somit auch zwei von den Zahlen

$$1, 2, 3, \dots, \frac{1}{2}(p-1)$$

für den Modul p kongruent, was unmöglich ist. Hätte man aber $p - a' \equiv a$, so würde daraus

$$a + a' \equiv 0 \pmod{p}$$

folgen; es wäre also die Summe zweier jener Produkte und somit auch die Summe zweier der Zahlen

$$1, 2, 3, \dots, \frac{1}{2}(p-1)$$

durch p teilbar, was ebenfalls unmöglich ist. Wenn wir also die Reste $a, b, c, d, \dots$ und die Ergänzungen der Reste $a', b', c', d', \dots$ zum Modul p , d. i.

$$p - a', p - b', p - c', p - d', \dots$$

zusammennnehmen, so werden wir, freilich in möglicherweise geänderter Reihenfolge, alle Zahlen

$$1, 2, 3, \dots, \frac{1}{2}(p-1)$$

erhalten. Wir setzen nun das Produkt dieser Zahlen gleich P ,

$$1.2.3 \dots \frac{1}{2}(p-1) = P,$$

dann wird

$$P = a b c d \dots \times (p - a')(p - b')(p - c')(p - d') \dots,$$

folglich

$$(-1)^n P = a b c d \dots \times (a' - p)(b' - p)(c' - p)(d' - p) \dots$$

sein.

Weiter ergibt sich für den Modul p

$$P M^{\frac{1}{2}(p-1)} \equiv a b c d \dots \times a' b' c' d' \dots$$

$$\equiv a b c d \dots \times (a' - p)(b' - p)(c' - p)(d' - p) \dots,$$

und somit ist

$$P M^{\frac{1}{2}(p-1)} \equiv P (-1)^n.$$

Hieraus folgt

$$M^{\frac{1}{2}(p-1)} \equiv \pm 1,$$

wo das obere oder das untere Zeichen zu nehmen ist, jenachdem n gerade oder ungerade ist. Bei Berücksichtigung des §. 109 folgt daraus ohne weiteres die Wahrheit des Satzes.

Beispiel. Um mit Hülfe dieses Satzes zu bestimmen, ob 6 ein Rest von 19 sei, bilden wir die Reste der neun ersten Vielfachen von 6. Es ist mod. 19

$$1.6 \equiv 6, 2.6 \equiv 12, 3.6 \equiv 18, 18 + 6 \equiv 5, 5 + 6 \equiv 11,$$

$$11 + 6 \equiv 17, 17 + 6 \equiv 4, 4 + 6 \equiv 10, 10 + 6 \equiv 16.$$

Von diesen neun Resten sind 12, 18, 11, 17, 10, 16 gröfser als $\frac{19}{2}$; in diesem Beispiel ist $n = 6$, also eine gerade Zahl, somit 6 Rest von 19.

§. 118.

Anwendungen des Gauss'schen Kriteriums.

Um den Nutzen des Gauss'schen Kriteriums zu zeigen, wollen wir mittels desselben zunächst die in §§. 115 und 116 bewiesenen Sätze nochmals herleiten und sodann einige weitere Anwendungen von demselben machen.

I. Um zu ermitteln, von welchen Primzahlen $-1 \equiv p-1$ quadratischer Rest ist, haben wir die kleinsten positiven Reste der Produkte

$$p-1, 2(p-1), 3(p-1), \dots, \frac{p-1}{2}(p-1),$$

das sind die Zahlen

$$p-1, p-2, p-3, \dots, \frac{p+1}{2}$$

zu betrachten. Dieselben sind sämtlich $> \frac{1}{2}p$, und ihre Anzahl beträgt $\frac{1}{2}(p-1)$. Da $\frac{1}{2}(p-1)$ gerade oder ungerade ist, jenachdem p die Form $4n+1$ oder $4n-1$ hat, so erhalten wir wieder das in §. 115 hergeleitete Resultat, dass -1 Rest der Primzahlen $4n+1$, Nichtrest der Primzahlen $4n+3$ ist.

II. Um zu bestimmen, von welchen Primzahlen 2 quadratischer Rest ist, haben wir zu untersuchen, wieviele der Zahlen

$$2, 4, 6, 8, \dots, p-1$$

grölser als $\frac{1}{2}p$ sind. Für die

Form von p	sind $< \frac{1}{2}p$ die Zahlen	$> \frac{1}{2}p$ die Zahlen
$8n+1$	$2, 4, 6, \dots, 4n$	$4n+2, \dots, 8n$
$8n+3$	$2, 4, 6, \dots, 4n$	$4n+2, \dots, 8n+2$
$8n+5$	$2, 4, 6, \dots, 4n+2$	$4n+4, \dots, 8n+4$
$8n+7$	$2, 4, 6, \dots, 4n+2$	$4n+4, \dots, 8n+6.$

Die Anzahl der letzteren beträgt für die verschiedenen Formen von p beziehungsweise

$$\frac{1}{2}(8n - 4n) = 2n, \quad \frac{1}{2}[(8n + 2) - 4n] = 2n + 1,$$

$$\frac{1}{2}[(8n + 4) - (4n + 2)] = 2n + 1,$$

$$\frac{1}{2}[(8n + 6) - (4n + 2)] = 2n + 2.$$

Da $2n$ und $2n + 2$ gerade sind, $2n + 1$ aber ungerade ist, so ergibt sich wie in §. 116, daß 2 Rest der Primzahlen

$$8n + 1 \quad \text{und} \quad 8n + 7,$$

Nichtrest der Primzahlen

$$8n + 3 \quad \text{und} \quad 8n + 5$$

ist.

In §. 127 wird noch ein dritter, höchst einfacher Beweis dieses wichtigen Satzes mitgeteilt werden.

III. Um zu bestimmen, von welchen Primzahlen 3 quadratischer Rest ist, haben wir die kleinsten positiven Reste der Zahlen

$$3, 6, 9, \dots, 3 \frac{(p-1)}{2}$$

zu nehmen. Jenachdem

$$p = 12n + 1, 5, 7, 11$$

ist, wird die letzte der zu betrachtenden Zahlen, d. i.

$$3 \frac{(p-1)}{2} = 18n \quad \text{oder} \quad = 18n + 6 \quad \text{oder} \quad = 18n + 9 \quad \text{oder} \\ = 18n + 15$$

sein. Wir schreiben jetzt jene Zahlen für jede der vier Formen des Moduls in der Weise in je drei Gruppen, daß die Zahlen der ersten Gruppe zwischen 0 und $\frac{1}{2}p$, die der zweiten zwischen $\frac{1}{2}p$ und p , die der dritten über p hinaus liegen:

Form des Moduls	Zahlen zwischen 0 und $\frac{p}{2}$	Zahlen zwischen $\frac{p}{2}$ und p
$12n + 1$	3, 6, ..., $6n$	$6n + 3$, ..., $12n$
$12n + 5$	3, 6, ..., $6n$	$6n + 3$, ..., $12n + 3$
$12n + 7$	3, 6, ..., $6n + 3$	$6n + 6$, ..., $12n + 6$
$12n + 11$	3, 6, ..., $6n + 3$	$6n + 6$, ..., $12n + 9$

Form des Moduls	Über p hinausliegende Zahlen	Kleinste positive Reste derselben
$12n + 1$	$12n + 3, \dots, 18n$	$2, 5, \dots, 6n - 1$
$12n + 5$	$12n + 6, \dots, 18n + 6$	$1, 4, \dots, 6n + 1$
$12n + 7$	$12n + 9, \dots, 18n + 9$	$2, 5, \dots, 6n + 2$
$12n + 11$	$12n + 12, \dots, 18n + 15$	$1, 4, \dots, 6n + 4.$

Da diese Reste sämtlich $< \frac{1}{2}p$ sind, so sind in jedem Falle nur die Zahlen der mittleren Gruppe $> \frac{1}{2}p$. Diese Gruppe enthält für

$$\begin{array}{l|l}
 p = 12n + 1 & \frac{1}{3} [12n - 6n] = 2n \\
 p = 12n + 5 & \frac{1}{3} [(12n + 3) - 6n] = 2n + 1 \\
 p = 12n + 7 & \frac{1}{3} [(12n + 6) - (6n + 3)] = 2n + 1 \\
 p = 12n + 11 & \frac{1}{3} [(12n + 9) - (6n + 3)] = 2n + 2
 \end{array}$$

Zahlen, und da $2n$ und $2n + 2$ gerade sind, $2n + 1$ aber ungerade ist, so erhalten wir den Satz: Die Zahl 3 ist quadratischer Rest der Primzahlen

$$12n + 1, \quad 12n + 11,$$

Nichtrest der Primzahlen

$$12n + 5, \quad 12n + 7.$$

Zusatz. Die Zahl -3 ist Rest der Primzahlen

$$12n + 1, \quad 12n + 7,$$

Nichtrest der Primzahlen

$$12n + 5, \quad 12n + 11.$$

Beweis. Für $p = 12n + 1$ ist

$$\left(\frac{3}{p}\right) = +1, \quad \left(\frac{-1}{p}\right) = +1,$$

folglich

$$\left(\frac{-3}{p}\right) = +1,$$

u. s. w.

Aufgabe. Es soll bewiesen werden, daß 5 Rest der Primzahlen

$$10n + 1, \quad 10n + 9,$$

Nichtrest der Primzahlen

$$10n + 3, \quad 10n + 7$$

ist.

Beweis. Die Zahlen

$$5, \quad 10, \quad 15, \quad \dots, \quad \frac{5(p-1)}{2}$$

sind, je nachdem sie zwischen 0 und $\frac{1}{2}p$, $\frac{1}{2}p$ und p , p und $\frac{3p}{2}$, $\frac{3p}{2}$ und $2p$, $2p$ und $\frac{5p}{2}$ liegen, in fünf Gruppen zu schreiben.

Die Zahlen der ersten Gruppe sind

$$< \frac{1}{2}p,$$

die kleinsten positiven Reste der dritten und fünften Gruppe ebenfalls. Die zweite Gruppe enthält, je nachdem p eine der vier angegebenen Formen hat, n , n , $n+1$, $n+1$ Zahlen, und diese sind sämtlich

$$> \frac{1}{2}p.$$

Ebenso enthält die vierte Gruppe beziehungsweise n , $n+1$, n , $n+1$ Zahlen, und die kleinsten positiven Reste derselben sind sämtlich

$$> \frac{1}{2}p.$$

Die zweite und vierte Gruppe enthalten also zusammen im ersten Fall $2n$, im zweiten $2n+1$, im dritten $2n+1$, im vierten $2n+2$ Zahlen, und daher ist 5 Rest im ersten und vierten, Nichtrest im zweiten und dritten Fall.

§. 119.

Der Reziprozitätssatz.

Wir wenden uns jetzt zu der dritten in §. 114 aufgestellten Frage: Von welchen ungeraden Primzahlen p ist eine andere



Carl Friedrich Gauss

(1777 — 1855).

Nach einer Lithographie des Jensen'schen Bildes.

ungerade Primzahl q Rest, und von welchen ist sie Nichtrest? Hierauf antwortet einer der wichtigsten Sätze der Zahlenlehre, der sogenannte Reziprozitätssatz, der sich folgendermaßen aussprechen läßt:

Wenn p und q zwei positive ungerade Primzahlen sind, von denen wenigstens eine die Form $4n + 1$ hat, so ist q Rest oder Nichtrest von p , jenachdem p Rest oder Nichtrest von q ist. Wenn aber jede der Primzahlen p, q die Form $4n + 3$ hat, so ist q Rest oder Nichtrest von p , jenachdem p Nichtrest oder Rest von q ist.

Dieser Satz ist zuerst von Euler (*Opuscula analytica* I, p. 84 = *Commentationes arithmet. collectae* I, p. 486), dann unabhängig davon von Legendre (*Théorie des Nombres* I, §. 6) durch Induktion gefunden worden. Erst Gauss gelang es, ihn vollständig zu beweisen. Gauss hat nacheinander sieben verschiedene Beweise des wichtigen Satzes gegeben (I. *Disquisitiones* 135; II. ebenda 262; III. Bd. II, p. 1; IV. Bd. II, p. 9; V. und VI. Bd. II, p. 47 ff.; VII. Bd. II, p. 234). Später sind noch andere Beweise gefunden worden. (Von Jacobi, Cauchy, Eisenstein, Liouville, Kronecker, Zeller, Schering u. a.) Eine vergleichende Darstellung dieser Beweise hat Oswald Baumgart in der Zeitschrift für Mathematik und Physik Bd. 30 veröffentlicht. Den von Eisenstein im 28. Bande des Crelleschen Journals gegebenen geometrischen Beweis habe ich in meine „Elemente der Zahlentheorie“ (Leipzig, 1887) aufgenommen. Der Anhang enthält eine graphische Darstellung des Satzes für die Primzahlen unter 100.

Bei Anwendung des Legendreschen Symbols läßt sich der Satz durch die Formel

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

ausdrücken. Wenn nämlich eine der Zahlen p, q die Form $4n + 1$ hat, so ist

$$\frac{p-1}{2} \cdot \frac{q-1}{2}$$

eine gerade Zahl, folglich hat die rechte Seite der Formel den Wert $+1$ und daher jedes der Symbole entweder den Wert $+1$

oder den Wert -1 . Wenn aber jede der Zahlen p, q von der Form $4n + 3$ ist, so ist

$$\frac{p-1}{2} \cdot \frac{q-1}{2}$$

ungerade, die rechte Seite der Formel also -1 , und daher muß in diesem Falle das eine der Symbole

$$\left(\frac{p}{q}\right), \quad \left(\frac{q}{p}\right)$$

gleich $+1$, das andere gleich -1 sein.

Wir beschränken uns hier auf den fünften der von Gauss gegebenen Beweise.

§. 120.

Beweis des Reziprozitätssatzes.

Es seien p und q zwei voneinander verschiedene positive ungerade Primzahlen. Wir bilden die kleinsten positiven Reste der Zahlen

$$q, \quad 2q, \quad 3q, \quad \dots, \quad \frac{1}{2}(p-1)q$$

für den Modul p ; die Anzahl derjenigen dieser Reste, die

$$> \frac{1}{2}p$$

sind, sei μ . Weiter bilden wir die kleinsten positiven Reste der Zahlen

$$p, \quad 2p, \quad 3p, \quad \dots, \quad \frac{1}{2}(q-1)p$$

für den Modul q ; die Anzahl derjenigen dieser Reste, die

$$> \frac{1}{2}q$$

sind, sei μ' . Dann ist nach dem Gauss'schen Kriterium q Rest von p , wenn μ gerade ist, p Rest von q , wenn μ' gerade ist.

Wir bezeichnen nun mit

f	den Komplex der Zahlen	$1, 2, 3, \dots, \frac{1}{2}(p-1),$
f'	" " " "	$p-1, p-2, p-3, \dots, \frac{1}{2}(p+1),$
F	" " " "	$1, 2, 3, \dots, \frac{1}{2}(q-1),$
F'	" " " "	$q-1, q-2, q-3, \dots, \frac{1}{2}(q+1).$

Dann zeigt die Zahl μ an, wieviele von den Zahlen qf ihre kleinsten positiven Reste für den Modul p in dem Komplex f' haben, und μ' zeigt an, wieviele der Zahlen pF ihre kleinsten positiven Reste für den Modul q in dem Komplex F' haben. Endlich soll noch

φ	den Komplex der Zahlen	$1, 2, 3, \dots, \frac{1}{2}(pq-1),$
φ'	" " " "	$pq-1, pq-2, pq-3, \dots, \frac{1}{2}(pq+1)$

bezeichnen.

Da jede durch p nicht teilbare ganze Zahl für den Modul p einem Rest aus f oder aus f' kongruent sein muß und jede durch q nicht teilbare ganze Zahl ebenso für den Modul q einem Rest aus F oder aus F' , so können die Zahlen φ , unter denen sich offenbar keine befindet, die zugleich durch p und durch q teilbar ist, in folgender Weise in acht Klassen geteilt werden:
Die Klasse

I soll die Zahlen enthalten, welche mod. p einer Zahl aus f und mod. q einer Zahl aus F kongruent sind. Die Anzahl dieser Zahlen sei $= \alpha$.

II soll die Zahlen enthalten, welche für die Moduln p, q beziehungsweise Zahlen aus f, F' kongruent sind. Die Anzahl dieser Zahlen sei $= \beta$.

III soll die Zahlen enthalten, welche für die Moduln p, q beziehungsweise Zahlen aus f', F kongruent sind. Ihre Anzahl sei $= \gamma$.

IV soll die Zahlen enthalten, welche für die Moduln p, q beziehungsweise Zahlen aus f', F' kongruent sind. Ihre Anzahl sei $= \delta$.

V soll die durch p teilbaren Zahlen enthalten, welche mod. q Zahlen aus F kongruent sind.

VI soll die durch p teilbaren Zahlen enthalten, welche mod. q Zahlen aus F' kongruent sind.

VII soll die durch q teilbaren Zahlen enthalten, welche mod. p Zahlen aus f kongruent sind.

VIII soll die durch q teilbaren Zahlen enthalten, welche mod. p Zahlen aus f' kongruent sind.

Offenbar enthalten die Klassen V und VI zusammen alle Zahlen pF , und da VI μ' Zahlen umfaßt, so befinden sich in V deren

$$\frac{1}{2} (q - 1) - \mu'.$$

Ebenso enthalten die Klassen VII und VIII zusammen alle Zahlen qf , und da die Anzahl der Zahlen von VIII gleich μ ist, so wird VII aus

$$\frac{1}{2} (p - 1) - \mu$$

Zahlen bestehen.

Auf ganz ähnliche Weise können wir alle Zahlen φ' in acht Klassen IX — XVI teilen. Wenn wir hierbei dieselbe Ordnung einhalten, so ist leicht zu sehen, daß die Zahlen der Klassen

IX, X, XI, XII, XIII, XIV, XV, XVI

beziehungsweise die Zahlen der Klassen

IV, III, II, I, VI, V, VIII, VII

zum Modul pq ergänzen, so daß sich in Klasse IX δ Zahlen vorfinden, in X γ Zahlen, u. s. w.

Vereinigt man alle Zahlen der I. mit allen Zahlen der IX. Klasse, so erhält man offenbar alle unterhalb pq liegenden Zahlen, die mod. p einer Zahl aus f , mod. q einer Zahl aus F kongruent sind, und man erkennt leicht, daß die Anzahl dieser Zahlen gleich der Anzahl der Kombinationen jeder der Zahlen f mit jeder der Zahlen F ist. Man erhält also

$$\alpha + \delta = \frac{1}{4} (p - 1)(q - 1).$$

Auf dieselbe Weise ergibt sich

$$\beta + \gamma = \frac{1}{4} (p - 1)(q - 1).$$

Durch Vereinigung aller Zahlen der Klassen II, IV, VI erhält man offenbar alle unterhalb $\frac{1}{2}pq$ liegenden Zahlen, die mod. q einer Zahl aus F' kongruent sind. Dieselben Zahlen können aber in folgender Weise dargestellt werden:

$F', q + F', 2q + F', 3q + F', \dots, \frac{1}{2}(p-3)q + F'$,
ihre Anzahl beträgt also

$$\frac{1}{4}(p-1)(q-1),$$

oder es ist

$$\beta + \delta + \mu' = \frac{1}{4}(p-1)(q-1).$$

Ebenso erhält man durch Vereinigung aller Zahlen der Klassen III, IV, VIII

$$\gamma + \delta + \mu = \frac{1}{4}(p-1)(q-1).$$

Aus den hergeleiteten vier Gleichungen ergeben sich die folgenden:

$$2\alpha = \frac{1}{4}(p-1)(q-1) + \mu + \mu',$$

$$2\beta = \frac{1}{4}(p-1)(q-1) + \mu - \mu',$$

$$2\gamma = \frac{1}{4}(p-1)(q-1) - \mu + \mu',$$

$$2\delta = \frac{1}{4}(p-1)(q-1) - \mu - \mu',$$

von denen jede die Wahrheit des Satzes beweist.

So oft nämlich jeder der beiden Moduln p, q oder einer derselben die Form $4n+1$ hat, ist

$$\frac{1}{4}(p-1)(q-1)$$

gerade, und daher müssen μ und μ' entweder beide gerade oder beide ungerade sein; die eine der Zahlen p, q ist dann also Rest oder Nichtrest der zweiten, je nachdem die zweite Rest oder Nichtrest der ersten ist. Wenn dagegen jede der Zahlen p, q die Form $4n+3$ hat, so ist

$$\frac{1}{4}(p-1)(q-1)$$

ungerade, folglich muß eine der Zahlen μ, μ' gerade, die andere ungerade sein, und dann ist q Rest oder Nichtrest von p , je nachdem p Nichtrest oder Rest von q ist.

Beispiele. I. Die Kongruenz

$$x^2 \equiv 35 \pmod{281}$$

ist möglich; denn es ist

$$\left(\frac{35}{281}\right) = \left(\frac{5}{281}\right) \cdot \left(\frac{7}{281}\right) = +1,$$

weil

$$\left(\frac{5}{281}\right) = \left(\frac{281}{5}\right) = \left(\frac{1}{5}\right) = +1$$

und

$$\left(\frac{7}{281}\right) = \left(\frac{281}{7}\right) = \left(\frac{1}{7}\right) = +1$$

ist.

$$\text{II. } \left(\frac{13}{941}\right) = \left(\frac{941}{13}\right) = \left(\frac{5}{13}\right) = \left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = -1.$$

$$\text{III. } \left(\frac{46}{509}\right) = \left(\frac{2}{509}\right) \left(\frac{23}{509}\right) = (-1)(+1) = -1;$$

es ist nämlich

$$\left(\frac{2}{509}\right) = -1,$$

weil

$$509 = 63 \cdot 8 + 5$$

ist; ferner ist

$$\left(\frac{23}{509}\right) = \left(\frac{509}{23}\right) = \left(\frac{3}{23}\right) = -\left(\frac{23}{3}\right) = -\left(\frac{2}{3}\right) = +1.$$

$$\text{IV. } \left(\frac{383}{443}\right) = -\left(\frac{60}{383}\right) = -\left(\frac{4}{383}\right) \left(\frac{3}{383}\right) \left(\frac{5}{383}\right) = +1;$$

denn

$$\left(\frac{4}{383}\right) = +1,$$

weil 4 eine Quadratzahl ist,

$$\left(\frac{3}{383}\right) = -\left(\frac{2}{3}\right) = +1,$$

$$\left(\frac{5}{383}\right) = \left(\frac{3}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

$$\text{V. } \left(\frac{443}{383}\right) = - \left(\frac{383}{443}\right) = -1.$$

$$\text{VI. } \left(\frac{-120}{2707}\right) = \left(\frac{-1}{2707}\right) \left(\frac{4}{2707}\right) \left(\frac{2}{2707}\right) \left(\frac{3}{2707}\right) \left(\frac{5}{2707}\right).$$

Nun ist

$$\left(\frac{-1}{2707}\right) = -1,$$

weil 2707 die Form $4n + 3$ hat;

$$\left(\frac{4}{2707}\right) = +1,$$

weil 4 eine Quadratzahl ist;

$$\left(\frac{2}{2707}\right) = -1,$$

weil 2707 die Form $8n + 3$ hat;

$$\left(\frac{3}{2707}\right) = -1,$$

weil 2707 die Form $12n + 7$ hat;

$$\left(\frac{5}{2707}\right) = -1,$$

da

$$\left(\frac{5}{2707}\right) = \left(\frac{2}{5}\right) = -1$$

ist. Wir erhalten somit

$$\left(\frac{-120}{2707}\right) = +1,$$

d. h. die Kongruenz

$$x^2 + 120 \equiv 0 \pmod{2707}$$

ist möglich. Ihre Wurzeln sind ± 341 .

§. 121.

Divisoren von $x^2 - a$ für den Fall, daß a eine Primzahl ist. (Gauss, Disquisitiones 147 ff.; Legendre, Théorie des Nombres, Bd. I, p. 261 und Tabellen III—VII.)

Wir sind jetzt imstande, allgemein zu bestimmen, für welche Primzahlen p als Moduln die Kongruenz $x^2 \equiv a$ möglich, und

für welche sie unmöglich ist. Zunächst setzen wir voraus, auch die gegebene Zahl a sei eine Primzahl, und da nach §. 116 die Kongruenz

$$x^2 \equiv 2 \pmod{p}$$

möglich oder unmöglich ist, jenachdem

$$p = 8n + 1 \quad \text{oder} \quad = 8n + 3$$

ist, so können wir den Fall $a = 2$ als abgethan und a als eine ungerade Primzahl ansehen. Eine solche kann von der Form $4n + 1$ oder von der Form $4n + 3$ und positiv oder negativ sein. Wir haben also vier Fälle zu behandeln.

I. Die gegebene Primzahl a sei positiv und von der Form $4n + 1$.

Die Kongruenz

$$x^2 \equiv a \pmod{p}$$

ist möglich, wenn

$$\left(\frac{a}{p}\right) = +1,$$

also nach dem Reziprozitätssatz auch

$$\left(\frac{p}{a}\right) = +1,$$

d. h. p quadratischer Rest von a ist. Bezeichnet man daher die Reste von a mit

$$r_1, \quad r_2, \quad r_3, \quad \dots,$$

die Nichtreste mit

$$n_1, \quad n_2, \quad n_3, \quad \dots,$$

und mit k eine unbestimmte ganze Zahl, so ist die Kongruenz

$$x^2 \equiv a \pmod{p}$$

möglich für alle Primzahlen der Formen

$$ak + r_1, \quad ak + r_2, \quad \dots,$$

unmöglich für alle Primzahlen der Formen

$$ak + n_1, \quad ak + n_2, \quad \dots,$$

oder, wenn wir uns der in §. 112 begründeten Ausdrucksweise bedienen: Die Formen der Divisoren von $x^2 - a$ sind

$$ak + r_1, \quad ak + r_2, \quad \dots,$$

die Formen der Nichtdivisoren

$$ak + n_1, \quad ak + n_2, \quad \dots$$

Beispiel. Da nach den Indizes-Tafeln 17 die Reste

1, 2, 4, 8, 9, 13, 15, 16,

die Nichtreste

3, 5, 6, 7, 10, 11, 12, 14

hat, so ergeben sich für $x^2 - 17$ als Formen der Divisoren

(1) $17k + 1, + 2, + 4, + 8, + 9, + 13, + 15, + 16,$

als Formen der Nichtdivisoren

(2) $17k + 3, + 5, + 6, + 7, + 10, + 11, + 12, + 14,$

d. h. die Kongruenz $x^2 \equiv 17$ ist möglich für alle Primzahlen der Formen (1), unmöglich für alle Primzahlen der Formen (2), oder anders ausgedrückt: Für jede Primzahl p einer jeden der Formen (1), aber für keine einzige Primzahl einer Form (2) läßt sich ein Wert von x finden, für welchen $x^2 - 17$ durch p teilbar wird. Unter 100 sind von den Formen (1) die Primzahlen

13, 19, 43, 47, 53, 59, 67, 83, 89,

von den Formen (2)

3, 5, 7, 11, 23, 29, 31, 37, 41, 61, 71, 73, 79, 97.

Man überzeuge sich durch Einsichtnahme der Tafeln, daß Ind. 17 für die ersteren Moduln gerade, für die letzteren ungerade ist.

Aufgabe. Die Zahl 7379 in Faktoren zu zerlegen.

Lösung. Man erhält durch Ausziehen der Quadratwurzel

$$7379 = 86^2 - 17.$$

Man hat also die Division von 7379 nur durch die Primzahlen zu versuchen, welche Divisoren von $x^2 - 17$ und < 86 sind. Die Divisionen durch 13, 19, 43 liefern einen Rest, die Division durch 47 nicht, und es ergibt sich

$$7379 = 47 \cdot 157.$$

II. Die gegebene Primzahl a sei negativ und von der Form $4n + 1$.

Die Kongruenz

$$x^2 \equiv -a$$

ist möglich, wenn

$$\left(\frac{-a}{p}\right), \text{ d. i. } \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = +1$$

ist, wenn also jedes der beiden Symbole

$$\left(\frac{-1}{p}\right), \left(\frac{a}{p}\right)$$

den Wert $+1$ oder den Wert -1 hat. Der Fall

$$\left(\frac{-1}{p}\right) = +1$$

setzt voraus, daß p die Form $4n+1$ habe und macht nach den vorhergehenden Entwicklungen keine Schwierigkeit. Wenn

$$\left(\frac{-1}{p}\right) = -1,$$

also p von der Form $4n+3$ ist, so muß, damit auch $\left(\frac{a}{p}\right)$ oder nach dem Reziprozitätssatz

$$\left(\frac{p}{a}\right) = -1$$

sei, p ein Nichtrest von a sein. Unter Beibehaltung der obigen Bezeichnungen der Reste und der Nichtreste von a ergibt sich also Folgendes: Die Divisoren von x^2+a sind alle Primzahlen $4n+1$ der Formen

$$ak + r_1, \quad ak + r_2, \quad \dots$$

und alle Primzahlen $4n+3$ der Formen

$$ak + n_1, \quad ak + n_2, \quad \dots;$$

Nichtdivisoren von x^2+a sind dagegen alle Primzahlen $4n+1$ der Formen

$$ak + n_1, \quad ak + n_2, \quad \dots$$

und alle Primzahlen $4n+3$ der Formen

$$ak + r_1, \quad ak + r_2, \quad \dots$$

Die beiden Bedingungen, daß eine Zahl für die Moduln 4 und a beziehungsweise die Reste 1 , resp. 3 und r , resp. n gebe, lassen sich nach §. 38 zusammenfassen.

Beispiel. Die Divisoren von x^2+17 sind die Primzahlen $4n+1$ der Formen

$$17k + 1, \quad 17k + 2, \quad \dots$$

und die Primzahlen $4n+3$ der Formen

$$17k + 3, \quad 17k + 5, \quad \dots,$$

oder, wenn beide Bedingungen vereinigt werden, die Primzahlen der Formen

$$68k + 1, 3, 7, 9, 11, 13, 21, 23, 25, 27, 31, 33, 39, 49, 53, 63.$$

Ebenso ergeben sich als Formen der Nichtdivisoren von $x^2 + 17$

$$68k + 5, 15, 19, 29, 35, 37, 41, 43, 45, 47, 55, 57, 59, 61, 65, 67.$$

Aufgabe. Die Zahl 6101 in Faktoren zu zerlegen.

Lösung. Es ist

$$6101 = 78^2 + 17,$$

und da die Divisionen durch

$$3, 7, 11, 13, 23, 31, 53, 71$$

sämtlich einen Rest geben, so ist 6101 eine Primzahl.

III. Die gegebene Primzahl a sei positiv und von der Form $4n + 3$.

Die Kongruenz

$$x^2 \equiv a \pmod{p}$$

ist möglich, wenn

$$\left(\frac{a}{p}\right) = +1$$

ist. Hat nun p die Form $4n + 1$, so ist das der Fall, wenn

$$\left(\frac{p}{a}\right) = +1,$$

also p Rest von a ist. Hat aber p die Form $4n + 3$, so wird nach dem Reziprozitätssatz, da dann

$$\left(\frac{a}{p}\right) = -\left(\frac{p}{a}\right)$$

ist,

$$\left(\frac{a}{p}\right) = +1$$

sein, wenn

$$\left(\frac{p}{a}\right) = -1,$$

also p Nichtrest von a ist. Es ergibt sich somit Folgendes:

Die Divisoren von $x^2 - a$ sind die Primzahlen $4n + 1$ der Formen

$$ak + r_1, \quad ak + r_2, \quad \dots$$

und die Primzahlen $4n + 3$ der Formen

$$ak + n_1, \quad ak + n_2, \quad \dots$$

Dagegen sind Nichtdivisoren die Primzahlen $4n + 1$ der Formen

$$ak + n_1, \quad ak + n_2, \quad \dots$$

und die Primzahlen $4n + 3$ der Formen

$$ak + r_1, \quad ak + r_2, \quad \dots$$

Beispiel. Die Zahl 23 hat die Reste

$$1, \quad 2, \quad 3, \quad 4, \quad 6, \quad 8, \quad 9, \quad 12, \quad 13, \quad 16, \quad 18,$$

die Nichtreste

$$5, \quad 7, \quad 10, \quad 11, \quad 14, \quad 15, \quad 17, \quad 19, \quad 20, \quad 21, \quad 22;$$

folglich sind die Divisoren von $x^2 - 23$ die Primzahlen $4n + 1$ der Formen

$$23k + 1, \quad 2, \quad 3, \quad \dots$$

und die Primzahlen $4n + 3$ der Formen

$$23k + 5, \quad 7, \quad \dots,$$

also, wenn wieder beide Bedingungen zusammengefaßt werden, die Primzahlen der Formen

$$92k + 1, \quad 7, \quad 9, \quad 11, \quad 13, \quad 15, \quad 19, \quad 25, \quad 29, \quad 41, \quad 43, \quad 49, \quad 51, \quad 63, \quad 67, \quad 73, \\ 77, \quad 79, \quad 81, \quad 83, \quad 85, \quad 91.$$

IV. Die gegebene Primzahl a sei negativ und von der Form $4n + 3$.

Die Kongruenz

$$x^2 \equiv -a \pmod{p}$$

ist möglich, wenn

$$\left(\frac{-a}{p}\right), \quad \text{d. i.} \quad \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = +1$$

ist. Hat nun p die Form $4n + 1$, so ist

$$\left(\frac{-1}{p}\right) = +1,$$

also erfordert die Möglichkeit der Kongruenz, daß

$$\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right) = +1$$

oder p Rest von a sei. Hat p die Form $4n + 3$, so ist

$$\left(\frac{-1}{p}\right) = -1,$$

also ist die Kongruenz nur dann möglich, wenn

$$\left(\frac{a}{p}\right) = -1$$

ist. Da jetzt sowohl a wie p die Form $4n + 3$ hat, so ist nach dem Reziprozitätssatz

$$\left(\frac{a}{p}\right) = -\left(\frac{p}{a}\right), \text{ also } \left(\frac{a}{p}\right) = -1,$$

wenn

$$\left(\frac{p}{a}\right) = +1$$

oder p ein Rest von a ist. Es ergibt sich somit Folgendes:

Die Divisoren von $x^2 + a$ sind die Primzahlen der Formen

$$ak + r_1, ak + r_2, \dots,$$

die Nichtdivisoren die Primzahlen der Formen

$$ak + n_1, ak + n_2, \dots$$

Beispiel. $x^2 + 23$ hat zu Divisoren die Primzahlen der Formen

$$23k + 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18,$$

zu Nichtdivisoren die Primzahlen der Formen

$$23k + 5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22.$$

Drückt man noch aus, daß die Primzahlen ungerade, also von der Form $2n + 1$ sein sollen, so erhält man als Formen der Divisoren

$$46k + 1, 3, 9, 13, 25, 27, 29, 31, 35, 39, 41,$$

als Formen der Nichtdivisoren

$$46k + 5, 7, 11, 15, 17, 19, 21, 33, 37, 43, 45.$$

§. 122.

Divisoren von $x^2 - A$ für den Fall, daß A eine zusammengesetzte Zahl ist.

Wir wollen jetzt die Formen der Divisoren und der Nichtdivisoren von $x^2 - A$ herleiten, indem wir unter A eine beliebig

zusammengesetzte Zahl verstehen. Zunächst leuchtet ein, daß wir nur die Werte von A zu berücksichtigen haben, welche durch keine Quadratzahl teilbar sind. Wenn nämlich $A = a^2 A'$ ist, so sind offenbar alle Divisoren von $x^2 - A$ (sofern sie prim zu A sind) auch Divisoren von $x^2 - A'$, und ebenso verhält es sich mit den Nichtdivisoren. Wir unterscheiden nun folgende drei Fälle:

I. A ist von der Form $+(4n + 1)$ oder $-(4n + 3)$.

II. A ist von der Form $-(4n + 1)$ oder $+(4n + 3)$.

III. A ist eine gerade Zahl oder von der Form $\pm(4n + 2)$.

I. A habe die Form $+(4n + 1)$ oder $-(4n + 3)$. Wir zerlegen A in seine Primfaktoren und geben jedem derselben, je nachdem er die Form $4n + 1$ oder $4n + 3$ hat, das Vorzeichen $+$ oder $-$. Da eine gerade Anzahl Faktoren der Form $4n + 3$ ein Produkt von der Form $4n + 1$ giebt, eine ungerade Anzahl ein Produkt von der Form $4n + 3$, so werden die Primfaktoren, auch nachdem sie in der angegebenen Weise mit Vorzeichen versehen sind, nicht aufhören, die vorgelegte Zahl A zum Produkt zu haben.

Die mit ihren Vorzeichen versehenen Primfaktoren von A seien $a, b, c, d, \dots$. Wir verteilen jetzt alle Zahlen, die prim zu A und $< A$ sind, in zwei Klassen. In die erste Klasse stellen wir die Zahlen, welche Nichtreste keines der Faktoren $a, b, c, d, \dots$ oder einer geraden Anzahl derselben sind, in die zweite Klasse die Zahlen, welche Nichtreste einer ungeraden Anzahl derselben sind. Werden die Zahlen der ersten Klasse mit $r_1, r_2, \dots$, die der zweiten Klasse mit $n_1, n_2, \dots$ bezeichnet, so sind

$$Ak + r_1, Ak + r_2, \dots$$

die Formen der Divisoren,

$$Ak + n_1, Ak + n_2, \dots$$

die Formen der Nichtdivisoren von $x^2 - A$, d. h. jede ungerade Primzahl wird Divisor oder Nichtdivisor von $x^2 - A$ sein, je nachdem sie in einer der ersteren oder in einer der letzten Formen enthalten ist.

Wenn nämlich p eine positive Primzahl und Rest oder Nichtrest einer der Zahlen $a, b, c, \dots$ ist, so wird diese letztere Zahl nach dem Reziprozitätssatz auch Rest oder Nichtrest von p sein. Wenn daher unter den Faktoren $a, b, c, \dots$ sich m befinden, deren Nichtrest p ist, so werden ebenso viele von ihnen Nicht-

reste von p sein. Ist also p in einer der ersteren Formen enthalten, so ist m gerade und A Rest von p . Wenn dagegen p in einer der letzteren Formen enthalten ist, so ist m ungerade, somit A Nichtrest von p .

Beispiel. Es sei

$$A = +105 = (-3)(+5)(-7).$$

Nichtreste keiner der Zahlen 3, 5, 7 sind:

$$1, 4, 16, 46, 64, 79.$$

Nichtreste von 3 sind:

$$2, 8, 11, 17, 23, 26, 29, 32, 38, 41, 44, 47, 53, 59, 62, 68, 71, 74, \\ 83, 86, 89, 92, 101, 104.$$

Nichtreste von 5 sind:

$$2, 17, 22, 32, 37, 47, 52, 62, 67, 82, 92, 97; 8, 13, 23, 38, 43, \\ 53, 58, 68, 73, 83, 88, 103.$$

Nichtreste von 7 sind:

$$17, 31, 38, 52, 59, 73, 94, 101; 19, 26, 47, 61, 68, 82, 89, 103; \\ 13, 34, 41, 62, 76, 83, 97, 104.$$

Folglich kommen in die

1. Klasse:

$$1, 4, 16, 46, 64, 79 \text{ (Nichtreste keiner der Zahlen 3, 5, 7),} \\ 2, 8, 23, 32, 53, 92 \text{ (Nichtreste von 3 und von 5),} \\ 26, 41, 59, 89, 101, 104 \text{ (Nichtreste von 3 und von 7),} \\ 13, 52, 73, 82, 97, 103 \text{ (Nichtreste von 5 und von 7).}$$

2. Klasse:

$$11, 29, 44, 71, 74, 86 \text{ (Nichtreste von 3 allein),} \\ 22, 37, 43, 58, 67, 88 \text{ (Nichtreste von 5 allein),} \\ 19, 31, 34, 61, 76, 94 \text{ (Nichtreste von 7 allein),} \\ 17, 38, 47, 62, 68, 83 \text{ (Nichtreste von 3, von 5 und von 7).}$$

Die Aufstellung der Formen der Divisoren und der Nichtdivisoren von $x^3 - 105$ hat danach keine Schwierigkeit.

II und III. Wir können diese beiden Fälle zusammen erledigen, indem wir

$$A = (\div 1) Q \text{ oder } = (+2) Q \text{ oder } = (-2) Q$$

setzen, wo Q eine Zahl von der Form

$$+ (4n + 1) \text{ oder } - (4n + 3)$$

ist, wie wir sie im ersten Fall betrachtet haben. Es sei allgemein $A = \alpha Q$, wo also

$$\alpha = -1 \text{ oder } = \pm 2$$

ist. Dann ist A Rest aller Zahlen, von denen entweder jede oder keine der beiden Zahlen α , Q Rest ist. Dagegen ist A Nichtrest aller Zahlen, von denen nur eine der beiden Zahlen α , Q Nichtrest ist. Danach lassen sich die Formen der Divisoren und der Nichtdivisoren von $x^2 - A$ leicht herleiten.

Es sei $\alpha = -1$. Wir verteilen alle Zahlen, die $< 4A$ und prim zu $4A$ sind, in zwei Klassen. In die erste Klasse stellen wir die Zahlen, welche in irgend einer Form der Divisoren von $x^2 - Q$ enthalten sind und zugleich die Form $4n + 1$ haben, sowie diejenigen, welche in einer Form der Nichtdivisoren von $x^2 - Q$ enthalten sind und zugleich die Form $4n + 3$ haben. In die zweite Klasse stellen wir die übrigen Zahlen. Sind $r_1, r_2, \dots$ die Zahlen der ersten, $n_1, n_2, \dots$ die Zahlen der zweiten Klasse, so ist A Rest aller Primzahlen der Formen

$$4Ak + r_1, 4Ak + r_2, \dots,$$

Nichtrest aller Primzahlen der Formen

$$4Ak + n_1, 4Ak + n_2, \dots$$

Wenn $\alpha = \pm 2$ ist, so verteilen wir alle Zahlen, die $< 8Q$ und prim zu $8Q$ sind, in zwei Klassen. In die erste Klasse stellen wir die Zahlen, welche in irgend einer Form der Divisoren von $x^2 - Q$ enthalten sind und zugleich für $\alpha = \pm 2$ eine der Formen

$$8n + 1, \quad 8n + 7,$$

für $\alpha = -2$ aber eine der Formen

$$8n + 1, \quad 8n + 3$$

haben; ferner diejenigen Zahlen, welche in irgend einer Form der Nichtdivisoren von $x^2 - Q$ enthalten sind und zugleich für $\alpha = \pm 2$ eine der Formen

$$8n + 3, \quad 8n + 5,$$

für $\alpha = -2$ dagegen eine der Formen

$$8n + 5, \quad 8n + 7$$

haben. In die zweite Klasse stellen wir alle übrigen Zahlen. Werden wieder die Zahlen der ersten Klasse mit $r_1, r_2, \dots$, diejenigen der zweiten Klasse mit $n_1, n_2, \dots$ bezeichnet, so ist $+2Q$ Rest aller Primzahlen der Formen

$$8Qk + r_1, 8Qk + r_2, \dots,$$

Nichtrest aller Primzahlen der Formen

$$8Qk + n_1, 8Qk + n_2, \dots$$

Der Beweis ist mit Hülfe des Reziprozitätssatzes und der in §. 115 und 116 hergeleiteten Sätze leicht zu führen.

Beispiel. Die Formen der Divisoren und der Nichtdivisoren von $x^2 + 15$ zu bestimmen.

Es ist

$$-15 = (-3)(+5).$$

Prim zu 15 und < 15 sind die Zahlen

$$1, 2, 4, 7, 8, 11, 13, 14.$$

Davon sind Nichtreste von $3:2$, 8, 11, 14, Nichtreste von $5:2$, 7, 8, 13.

Es kommen also in die

Klasse I: 1, 2, 4, 8;

Klasse II: 7, 11, 13, 14.

Folglich sind die Formen der Divisoren von $x^2 + 15$

$$15k + 1, 2, 4, 8,$$

die Formen der Nichtdivisoren

$$15k + 7, 11, 13, 14,$$

oder, wenn man ausdrückt, daß die Zahlen sowohl die Form $4n + 1$, als auch die Form $4n + 3$ haben können, es sind die Formen der Divisoren

$$60k + 1, 17, 19, 23, 31, 47, 49, 53,$$

die der Nichtdivisoren

$$60k + 7, 11, 13, 29, 37, 41, 43, 59.$$

Um jetzt die Formen der Divisoren und der Nichtdivisoren von $x^2 - 15$ zu finden, haben wir die 16 Zahlen, die prim zu 60 und < 60 sind, in der oben angegebenen Weise in zwei

Klassen zu teilen. Dann ergeben sich als Formen der Divisoren von $x^2 - 15$

$$60k + 1, 7, 11, 17, 43, 49, 53, 59,$$

als Formen der Nichtdivisoren

$$60k + 13, 19, 23, 29, 31, 37, 41, 47.$$

Im Anhang sind die Formen der Divisoren von $x^2 \pm a$ für die Werte von $a = 1$ bis $a = 23$ angegeben.

§. 123.

Auflösung der rein quadratischen Kongruenz

Nachdem wir gelernt haben zu entscheiden, ob eine Kongruenz

$$x^2 \equiv a \pmod{m}$$

möglich sei oder nicht, handelt es sich darum, die Wurzeln einer als möglich erkannten Kongruenz zu bestimmen. Eine naheliegende Art der Auflösung haben wir schon in §. 103 kennen gelernt. Nach derselben bildet man die Reihe¹⁾

$$a, a + m, a + 2m, \dots$$

Jede Quadratzahl μ^2 , welche sich in dieser Reihe vorfindet, giebt ein Wurzelpaar

$$x \equiv \pm \mu \pmod{m}$$

der Kongruenz

$$x^2 \equiv a \pmod{m}.$$

Wir wollen jetzt untersuchen, wie weit man die Reihe fortzusetzen hat, um alle Wurzeln zu erhalten. Da

$$x \leq \frac{1}{2} m$$

vorausgesetzt werden darf, so ist

$$x^2 \leq \frac{1}{4} m^2,$$

¹⁾ Eine bedeutende Verbesserung hat diese Methode durch Gauss erfahren, der (Disquisitiones 319 ff.) lehrt, wie man von den Gliedern dieser Reihe möglichst viele, die keine Lösung geben können, von vornherein ausschließt. Eine einfache Darstellung dieser Ausschließungsmethode findet der Leser in §. 91 meiner „Elemente der Zahlentheorie“ (Leipzig, 1887).

also, wenn $a + km$ das letzte in Betracht zu ziehende Glied der Reihe bezeichnet,

$$a + km \leq \frac{1}{4} m^2.$$

Wird nun a als positiv vorausgesetzt, so ist

$$km < \frac{1}{4} m^2,$$

folglich

$$k < \frac{1}{4} m.$$

Wenn a negativ ist, so wird der Grenzwert $\frac{1}{4} m$ von k , da der absolute Wert von a kleiner als m ist, um höchstens eine Einheit erhöht. Durch Prüfung der $1 + E\left(\frac{m}{4}\right)$ ersten Glieder der Reihe findet man also für ein positives a alle Wurzeln der Gleichung. Bei einem negativen a ist noch ein Glied mehr zu nehmen. $E\left(\frac{m}{4}\right)$ bezeichnet die größte ganze Zahl, die in dem Bruche $\frac{m}{4}$ enthalten ist.

Beispiel. Die Kongruenz $x^2 \equiv 4 \pmod{105}$ zu lösen, bilden wir die Reihe

4, 109, 214, 319, 424, 529, 634, 739, 844, 949, 1054, 1159, 1264, 1369, 1474, 1579, 1684, 1789, 1894, 1999, 2104, 2209, 2314, 2419, 2524, 2629.

Dieselbe enthält die Quadratzahlen 4, 529, 1369, 2209, also hat die Kongruenz die acht Wurzeln

$$x \equiv \pm 2, \pm 23, \pm 37, \pm 47 \pmod{105}.$$

Statt des dargelegten Verfahrens¹⁾ kann man sich in vielen Fällen einer direkten Lösungsmethode bedienen. Nach §. 112 dürfen wir voraussetzen, daß der Modul eine Potenz einer ungeraden Primzahl sei; denn der Fall $m = 2^r$ ist in §. 111 behandelt worden. Da außerdem in §. 107 gezeigt worden ist, wie man aus den Wurzeln von $x^2 \equiv a \pmod{p}$ diejenigen von

¹⁾ Daß die rein quadratische Kongruenz auch dem oben für die allgemeine binomische Kongruenz gelehrteten Lösungsverfahren unterliegt, braucht hier wohl nur erwähnt zu werden.

$x^2 \equiv a \pmod{p^1}$ berechnet, so können wir uns auf den Fall beschränken, in welchem der Modul eine ungerade Primzahl p ist. Am einfachsten gestaltet sich die Sache, wenn p die Form $4n + 3$ hat. Ist aber $p = 4n + 1$, so wird der Weg, der für $p = 8n + 5$ zum Ziele führen kann, für $p = 8n + 1$ nicht anwendbar sein. Wir haben also drei Fälle zu unterscheiden, die wir der Reihe nach besprechen wollen.

I. Es sei

$$p = 4n + 3.$$

Wenn die Kongruenz

$$x^2 \equiv a \pmod{p}$$

möglich, also a Rest von p sein soll, so muß nach §. 109

$$a^{\frac{1}{2}(p-1)}, \text{ d. i. } a^{2n+1} \equiv 1 \pmod{p},$$

folglich

$$a^{2n+2}, \text{ d. i. } (a^{n+1})^2 \equiv a \pmod{p}$$

sein. Die Wurzeln der Kongruenz sind dann also

$$x \equiv \pm a^{n+1} \pmod{p}.$$

Beispiel. Die Kongruenz

$$x^2 \equiv 35 \pmod{59 = 4 \cdot 14 + 3}$$

hat die Wurzeln

$$x \equiv \pm 35^{14} \equiv \pm 25 \pmod{59}.$$

II. Es sei

$$p = 8n + 5.$$

Wenn a Rest von p sein soll, so muß

$$a^{\frac{1}{2}(p-1)}, \text{ d. i. } a^{4n+2} \equiv 1,$$

folglich

$$a^{4n+2} - 1 = (a^{2n+1} - 1)(a^{2n+1} + 1) \equiv 0 \pmod{p}$$

sein.

Wenn nun erstens

$$a^{2n+1} - 1 \equiv 0 \pmod{p}$$

ist, so ergibt sich

$$a^{2n+2}, \text{ d. i. } (a^{n+1})^2 \equiv a \pmod{p}.$$

In diesem Falle hat also die vorgelegte Kongruenz die beiden Wurzeln

$$x \equiv \pm a^{n+1} \pmod{p}.$$

Wenn zweitens

$$a^{2n+1} + 1 \equiv 0 \pmod{p}$$

ist, so bleibt nichts anderes übrig, als in der oben dargelegten Weise die Lösung mittels der Reihe $a, a + p, \dots$ zu suchen, es müßte denn sein, daß man die beiden Quadratzahlen kennt, deren Summe $= p$ ist. (Die Zerfällung von p in zwei Quadrate setzt die Lösung der Kongruenz

$$x^2 \equiv -1 \pmod{p}$$

voraus, kann also nicht zur Grundlage der Lösung von

$$x^2 \equiv a \pmod{p}$$

dienen.) Man hat nämlich

$$a^{2n+2} + a \equiv 0,$$

also weil $a \equiv x^2$ ist,

$$(a^{n+1})^2 + x^2 \equiv 0 \pmod{p}.$$

Ist nun $p = \alpha^2 + \beta^2$, wo α und β relative Primzahlen sind, und bezeichnen t, u zwei unbestimmte ganze Zahlen, so ist auch

$$(\alpha^2 + \beta^2)(t^2 + u^2)$$

oder, was dasselbe ist,

$$(\alpha t + \beta u)^2 + (\alpha u - \beta t)^2 \equiv 0 \pmod{p}.$$

Wir verfügen jetzt über t, u so, daß

$$\alpha u - \beta t \equiv a^{n+1}$$

$$\beta u + \alpha t \equiv x$$

werde. Hieraus erhält man durch Elimination von u

$$(\alpha^2 + \beta^2)t \equiv \alpha x - \beta a^{n+1},$$

also, weil

$$\alpha^2 + \beta^2 = p \equiv 0 \pmod{p}$$

ist,

$$\alpha x \equiv \beta a^{n+1} \pmod{p}.$$

Diese Kongruenz ersten Grades ist immer möglich, da α prim zu p ist. Sie liefert einen einzigen Wert von x , der des doppelten Vorzeichens wegen die beiden Wurzeln der Kongruenz

$$x^2 \equiv a \pmod{p}$$

darstellt.

Beispiele.

$$\text{I. } x^2 \equiv 15 \pmod{61 = 7 \cdot 8 + 5}.$$

Da

$$15^{2 \cdot 7 + 1} = 15^{15} \equiv +1 \pmod{61}$$

ist, so sind die Wurzeln

$$x \equiv \pm 15^{7+1} \equiv \pm 15^8 \equiv \pm 25 \pmod{61}.$$

$$\text{II. } x^2 \equiv 5 \pmod{61}.$$

Es ist

$$5^{15} \equiv -1 \pmod{61} \quad \text{und} \quad 61 = 5^2 + 6^2,$$

folglich hat man die Kongruenz

$$5x \equiv 6 \cdot 5^8 \pmod{61}$$

zu lösen. Es ergibt sich

$$x \equiv 6 \cdot 5^7 \equiv \pm 26 \pmod{61}.$$

[Man hätte auch die Kongruenz

$$6x \equiv 5 \cdot 5^8 \equiv 5^9 \pmod{61}$$

nehmen können; diese würde

$$x \equiv \pm 35 \pmod{61},$$

also dasselbe Resultat geliefert haben.]

III. Wenn $p = 8n + 1$ ist, hat man sich in der Regel des im Anfang dieses Paragraphen dargelegten Verfahrens zu bedienen. Es kann aber auch in diesem Falle vorkommen, daß sich die Wurzeln der Kongruenz $x^2 \equiv a \pmod{p}$ direkt bestimmen lassen. Es sei nämlich $p = 2^x q + 1$, wo $x \leq 3$ und q eine ungerade Zahl ist. Da die Kongruenz möglich sein soll, so ist

$$a^{\frac{1}{2}(p-1)} = a^{2^{x-1}q} \equiv 1 \pmod{p}.$$

Wenn sich nun herausstellt, daß schon

$$a^q \equiv \pm 1 \pmod{p}$$

ist, so können wir, weil q ungerade ist, ganz wie im Falle

$$p = 8n + 5$$

verfahren.

Beispiele.

$$\text{I. } x^2 \equiv 17 \pmod{89 = 8 \cdot 11 + 1}.$$

Da

$$17^{11} \equiv -34 \pmod{89}$$

ist, so läßt sich ein direktes Verfahren nicht anwenden. Die Betrachtung der Reihe

$$17, 106, 195, 284, \dots$$

liefert als Wurzeln

$$x \equiv \pm 27 \pmod{89}.$$

$$\text{II. } x^2 \equiv 71 \pmod{73} = 8 \cdot 9 + 1.$$

Es ist

$$71^9 \equiv (-2)^9 \equiv -512 \equiv -1 \pmod{73}$$

und

$$73 = 3^2 + 8^2.$$

Man erhält also zur Bestimmung von x

$$8x \equiv 3 \cdot 71^5 \equiv 3 \cdot (-2)^5 \equiv -96 \pmod{73}$$

und daraus

$$x \equiv \pm 12 \pmod{73}.$$

§. 124.

Die Kongruenz $x^2 \equiv a \pmod{m}$, wenn a nicht prim zu m ist.

Des leichteren Verständnisses wegen möge der allgemeinen Betrachtung ein Beispiel vorausgeschickt werden. Es soll die Kongruenz

$$x^2 \equiv 450 \pmod{525}$$

gelöst werden. Da 450 und 525 den größten gemeinschaftlichen Divisor 75 haben, so muß auch x^2 durch $75 = 3 \cdot 5^2$, also x durch $3 \cdot 5 = 15$ teilbar sein. Wir setzen demgemäß $x = 15y$ und erhalten der Reihe nach

$$225y^2 \equiv 450 \pmod{525},$$

$$3y^2 \equiv 6 \pmod{7},$$

$$y^2 \equiv 2 \pmod{7},$$

$$y \equiv \pm 3 \pmod{7},$$

$$x \equiv \pm 45 \pmod{105}.$$

Die Kongruenz hat also die 10 verschiedenen Wurzeln

$$x \equiv \pm 45, \pm 150, \pm 255, \pm 360, \pm 465 \pmod{525}.$$

Es sei jetzt die Kongruenz

$$(1) \quad x^2 \equiv a \pmod{m}$$

vorgelegt. Wenn a und m den grössten gemeinschaftlichen Divisor $d^2 \delta$ haben, wo d^2 die grösste in diesem Divisor aufgehende Quadratzahl bezeichnen möge, so muß x^2 durch $d^2 \delta$, also x durch $d \delta$ teilbar sein. Wir setzen demgemäss $x = d \delta y$ und erhalten

$$d^2 \delta^2 y^2 \equiv a \pmod{m}$$

oder

$$(2) \quad \delta y^2 \equiv \frac{a}{d^2 \delta} \pmod{\frac{m}{d^2 \delta}},$$

wo

$$\frac{a}{d^2 \delta} \quad \text{und} \quad \frac{m}{d^2 \delta}$$

teilerfremde ganze Zahlen sind. Es läßt sich nun zeigen, daß δ prim zu $\frac{m}{d^2 \delta}$ sein wird. Hätten beide Zahlen einen Faktor $\delta_1 > 1$ gemeinschaftlich, so müßte derselbe auch in $d \delta y = x$ aufgehen, x^2 also durch δ_1^2 teilbar sein. Es wäre aber auch m durch δ_1^2 teilbar, da δ_1 in $\frac{m}{d^2 \delta}$, also δ_1^2 in $\frac{m}{d^2}$ und somit in m aufgeht. Folglich könnte die Kongruenz (1) nur bestehen, wenn auch a durch δ_1^2 teilbar wäre. Der grösste gemeinschaftliche Divisor von a und m enthielte also den quadratischen Faktor $d^2 \delta_1^2$, während vorausgesetzt wird, daß die grösste in diesem Divisor aufgehende Quadratzahl d^2 sei. Somit ist der Koeffizient δ von y^2 in (2) prim zum Modul dieser Kongruenz. Dieselbe liefert also für y^2 nur einen Wert und führt zu einer rein quadratischen Kongruenz, die nach §. 123 zu behandeln ist. Nachdem man die Werte von y gefunden hat, macht die Bestimmung der Werte von x keine Schwierigkeit mehr.

Beispiel. $x^2 \equiv 819 \pmod{3150}$.

$$819 = 3^2 \cdot 7 \cdot 13, \quad 3150 = 2 \cdot 3^2 \cdot 5^2 \cdot 7, \quad d = 3^2 \cdot 7.$$

Wir setzen $x = 21y$, dann erhalten wir

$$3^2 \cdot 7^2 \cdot y^2 \equiv 3^2 \cdot 7 \cdot 13 \pmod{2 \cdot 3^2 \cdot 5^2 \cdot 7}$$

oder

$$7y^2 \equiv 13 \pmod{50},$$

$$y^2 \equiv 9 \pmod{50},$$

$$y \equiv \pm 3 \pmod{50},$$

$$x \equiv \pm 63 \pmod{1050}.$$

Die vorgelegte Kongruenz hat also die Wurzeln

$$x \equiv +63, \quad +1113, \quad +2163 \pmod{3150}.$$

§. 125.

Über die Aufeinanderfolge der Reste und Nichtreste der Primzahl p in der Reihe $1, 2, 3, \dots, p - 1$.

Es bezeichne R_r , wie oft in der Reihe

$$(1) \quad 1, 2, 3, \dots, p - 1$$

auf einen Rest von p ein Rest folgt. Ebenso werde durch

$$R_n, \quad N_r, \quad N_n$$

ausgedrückt, wie oft in (1) beziehungsweise auf einen Rest ein Nichtrest, auf einen Nichtrest ein Rest, auf einen Nichtrest ein Nichtrest folgt. Dann ist offenbar

$$(2) \quad R_r + R_n + N_r + N_n = p - 2.$$

Ist nun α ein Nichtrest der Reihe (1) und wird eine zweite (von α verschiedene) Zahl β so bestimmt, daß

$$\alpha\beta \equiv 1 \pmod{p}$$

ist, so muß auch β ein Nichtrest sein. Wäre nun eine der Zahlen α, β , etwa $\beta = p - 1$, also

$$\alpha(p - 1) \equiv 1 \pmod{p},$$

so müßte $-\alpha \equiv 1$, also auch

$$\alpha \equiv -1 \equiv p - 1$$

sein, was der Voraussetzung, nach welcher α von β verschieden sein soll, widerspricht. Da nun β als Glied von (1) vorausgesetzt werden darf, so ist sowohl α als auch $\beta < p - 1$. Wir betrachten jetzt die beiden Folgen

$$\alpha, \alpha + 1 \quad \text{und} \quad \beta, \beta + 1.$$

Wenn $\alpha + 1$ ein Nichtrest ist, so muß

$$\beta + 1 \equiv \beta + \alpha\beta \equiv \beta(\alpha + 1)$$

als Produkt zweier Nichtreste ein Rest sein. Wenn also die Folge $\alpha, \alpha + 1$ eine Einheit für N_n liefert, so liefert $\beta, \beta + 1$ eine Einheit für N_r .

Ist dagegen $\alpha + 1$ ein Rest, so wird $\beta + 1 \equiv \beta(\alpha + 1)$ als Produkt eines Nichtrestes in einen Rest ein Nichtrest sein.

So oft also die Folge $\alpha, \alpha + 1$ eine Einheit für N_r liefert, liefert $\beta, \beta + 1$ eine Einheit für N_n . Daher ist in allen Fällen

$$(3) \quad N_r = N_n.$$

Um nun die Größen

$$R_r, R_n, N_r, N_n$$

einzelnen zu berechnen, haben wir die Fälle

$$p = 4n + 1 \quad \text{und} \quad p = 4n + 3$$

gesondert zu behandeln.

I. Wenn $p = 4n + 1$ ist, so ist nach §. 115 $p - 1$ ein Rest und $p - m$ Rest oder Nichtrest, jenachdem m Rest oder Nichtrest ist.

Ist nun α ein Rest und $\alpha + 1$ ein Nichtrest, so wird $p - \alpha - 1$ ein Nichtrest, $p - \alpha$ ein Rest sein. Jeder durch die Folge $\alpha, \alpha + 1$ gelieferten Einheit von R_n entspricht also eine durch die Folge $p - \alpha - 1, p - \alpha$ gelieferte Einheit von N_r . In diesem Falle ist somit

$$(4) \quad R_n = N_r.$$

Da es ferner $\frac{1}{2}(p - 1)$ Reste und ebenso viele Nichtreste gibt, und da auf jeden Nichtrest entweder ein Rest oder ein Nichtrest und auf jeden Rest — mit Ausnahme des letzten, nämlich des Restes $p - 1$ — gleichfalls entweder ein Rest oder ein Nichtrest folgt, so ist weiter

$$(5) \quad \begin{cases} N_r + N_n = \frac{1}{2}(p - 1) \\ R_r + R_n = \frac{1}{2}(p - 1) - 1. \end{cases}$$

Aus (3), (4) und (5) erhält man

$$(6) \quad R_r = \frac{1}{4}(p - 5), \quad R_n = N_r = N_n = \frac{1}{4}(p - 1).$$

II. Wenn $p = 4n + 3$ ist, so ist nach §. 115 $p - 1$ ein Nichtrest, und m und $p - m$ sind von entgegengesetztem quadratischen Charakter.

Wenn also α ein Nichtrest und $\alpha + 1$ ebenfalls ein Nichtrest ist, so daß die Folge $\alpha, \alpha + 1$ eine Einheit für N_n liefert, so wird $p - \alpha - 1$ ebenso wie $p - \alpha$ ein Rest sein, die

Folge $p - \alpha - 1$, $p - \alpha$ somit eine Einheit für R_r liefern. Es ist folglich

$$(7) \quad N_n = R_r.$$

Da ferner in diesem Falle

$$(8) \quad \begin{cases} R_r + R_n = \frac{1}{2} (p - 1) \\ N_r + N_n = \frac{1}{2} (p - 1) - 1 \end{cases}$$

ist, so erhalten wir [aus (3), (7), und (8)]

$$(9) \quad R_r = N_r = N_n = \frac{1}{4} (p - 3), \quad R_n = \frac{1}{4} (p + 1).$$

Die Ausdrücke (6) und (9) lassen erkennen, daß jede der Zahlen

$$R_r, R_n, N_r, N_n$$

einen von Null verschiedenen Wert hat, sobald die Primzahl $p > 5$ ist.

Beispiele.

I. $p = 23$.

$$\begin{array}{cccccccccccccccccc} 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8, & 9, & 10, & 11, & 12, & 13, & 14, & 15, \\ + & + & + & + & - & + & - & + & + & - & - & + & + & - & - \\ 16, & 17, & 18, & 19, & 20, & 21, & 22. \\ + & - & + & - & - & - & - \end{array}$$

$$R_r = 5, \quad R_n = 6, \quad N_r = 5, \quad N_n = 5.$$

II. $p = 29$.

$$\begin{array}{cccccccccccccccccccccc} 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8, & 9, & 10, & 11, & 12, & 13, & 14, & 15, \\ + & - & - & + & + & + & + & - & + & - & - & - & + & - & - \\ 16, & 17, & 18, & 19, & 20, & 21, & 22, & 23, & 24, & 25, & 26, & 27, & 28. \\ + & - & - & - & + & - & + & + & + & + & - & - & + \end{array}$$

$$R_r = 6, \quad R_n = 7, \quad N_r = 7, \quad N_n = 7.$$

Anmerkung. Wird statt (1) die Reihe

$$(10) \quad c, \quad 2c, \quad 3c, \quad \dots, \quad (p-1)c$$

genommen, wo c eine beliebige durch p nicht teilbare Zahl bezeichnet, so sind zwei entsprechende Glieder von (1) und (10) von demselben oder von entgegengesetztem quadratischen Charakter, je nachdem c Rest oder Nichtrest von p ist.

§. 126.

Auflösung der Kongruenz $ax^2 + by^2 \equiv c \pmod{p}$.

Hilfssatz. Wenn a prim zu m ist, so ist die Kongruenz

$$ax^2 \equiv b \pmod{m}$$

möglich oder unmöglich, jenachdem a und b in Beziehung auf den Modul m von demselben oder von entgegengesetztem quadratischen Charakter sind.

Beweis. Da a prim zu m ist, so läßt sich stets eine, aber auch nur eine Zahl α bestimmen, für welche

$$a\alpha \equiv 1 \pmod{m}$$

ist. α wird von demselben quadratischen Charakter wie a sein, da das Produkt $a\alpha$ ein Rest, nämlich $+1$ ist. α wird auch prim zu m sein, da ein gemeinschaftlicher Divisor von α und m in 1 aufgehen müßte. Wird nun die Kongruenz

$$ax^2 \equiv b \pmod{m}$$

mit α multipliziert, so erhält man

$$x^2 \equiv \alpha b \pmod{m},$$

und damit diese letztere Kongruenz möglich, d. i. αb ein Rest sei, müssen α und b oder, was dasselbe ist, a und b denselben quadratischen Charakter in Beziehung auf m haben.

Wenn danach die Koeffizienten b und c der Kongruenz

$$ax^2 + by^2 \equiv c \pmod{p},$$

in welcher der Rest c als von Null verschieden vorausgesetzt wird, von demselben quadratischen Charakter in Beziehung auf p sind, so ist die Kongruenz

$$by^2 \equiv c \pmod{p}$$

möglich und liefert für y zwei Werte, welche in Verbindung mit dem Werte $x = 0$ zwei Lösungen der vorgelegten Kongruenz ausmachen.

Haben a und c denselben quadratischen Charakter, so kann man $y = 0$ annehmen und die zugehörigen Werte von x durch die Kongruenz $ax^2 \equiv c \pmod{p}$ bestimmen.

Um die übrigen Lösungen zu erhalten, bilden wir die Reihe der Vielfachen von $-c \equiv p - c$

$$p - c, 2(p - c), 3(p - c), \dots, (p - 1)(p - c)$$

und wählen zwei aufeinander folgende Glieder dieser Reihe, α und $\alpha + (p - c)$, von denen das erste, α , von demselben quadratischen Charakter wie a , das zweite, d. i. $\alpha + p - c$, von demselben quadratischen Charakter wie $-b$ ist. Für jedes Paar solcher Werte $\alpha, \alpha + p - c$ liefern dann die Kongruenzen

$$ax^2 \equiv \alpha, \quad -by^2 \equiv \alpha + (p - c) \pmod{p}$$

Werte von x und y , welche die vorgelegte Kongruenz befriedigen; denn da

$$+by^2 \equiv -\alpha + c \quad \text{und} \quad ax^2 \equiv \alpha$$

ist, so ist

$$ax^2 + by^2 \equiv c \pmod{p}.$$

Wir haben noch zu zeigen, daß alle Lösungen auf die dargelegte Weise erhalten werden.

Es sei

$$x = \xi, \quad y = \eta$$

eine Lösung der vorgelegten Kongruenz, also

$$-a\xi^2 - b\eta^2 \equiv -c \equiv p - c \pmod{p}.$$

Da nun die Reihe der Vielfachen von $p - c$

$$p - c, 2(p - c), 3(p - c), \dots, (p - 1)(p - c)$$

alle Reste und Nichtreste von 1 bis $p - 1$ enthält, so müssen $-b\eta^2$ und $+a\xi^2$, deren Differenz (ebenso wie die Differenz der Reihe) gleich $p - c$ ist, zwei aufeinander folgenden Vielfachen von $p - c$ kongruent sein.

Beispiele.

$$\text{I. } 7x^2 + 5y^2 \equiv 22 \pmod{23}.$$

Da 5, 7, 22 Nichtreste von 23 sind, so lösen wir zunächst die Kongruenz

$$7x^2 \equiv 22 \pmod{23}$$

und erhalten $x \equiv \pm 6$. Weiter liefert die Kongruenz

$$5y^2 \equiv 22 \pmod{23}$$

die Werte $y \equiv \pm 3$. Die vorgelegte Kongruenz hat also die Lösungen

$$\pm x \equiv 6, \quad \pm y \equiv 0 \quad \text{und} \quad \pm x \equiv 0, \quad \pm y \equiv 3 \pmod{23}.$$

Um die übrigen Lösungen zu erhalten, bilden wir die Vielfachen von $23 - 22 = 1$ und schreiben wieder der Deutlichkeit wegen unter jeden Rest das Zeichen $+$, unter jeden Nichtrest das Zeichen $-$.

1,	2,	3,	4,	5,	6,	7,	8,	9,	10,	11,	12,	13,	14,	15,
+	+	+	+	-	+	-	+	+	-	-	+	+	-	-
16, 17, 18, 19, 20, 21, 22.														
+ - + - - - -														

Da 7 Nichtrest, $-5 \equiv 18$ Rest ist, so haben wir die Zeichenfolge $- +$ zu nehmen, also die Kongruenzen

$7x^2 \equiv 5$	7	11	15	17
$18y^2 \equiv 6$	8	12	16	18

zu lösen, und diese liefern

$\pm x \equiv 2$	1	8	9	3
$\pm y \equiv 10$	7	4	12	1.

$$\text{II. } 6x^2 + 11y^2 \equiv 14 \pmod{29}.$$

Da 6 Rest, 11 Nichtrest und 14 Nichtrest von 29 ist, so ist die Annahme $y \equiv 0$ unzulässig. Es kann aber $x \equiv 0$ und dabei

$$11y^2 \equiv 14 \pmod{29}$$

sein, was $y \equiv \pm 5$ liefert. Das erste Lösungspaar ist also

$$x \equiv 0, \quad y \equiv \pm 5.$$

Um die übrigen Lösungen zu erhalten, bilden wir die Vielfachen von $29 - 14 = 15$:

15,	1,	16,	2,	17,	3,	18,	4,	19,	5,	20,	6,	21,	7,	22,
-	+	+	-	-	-	-	+	-	+	+	+	-	+	+
8, 23, 9, 24, 10, 25, 11, 26, 12, 27, 13, 28, 14.														
- + + + - + - - - - + + -														

Da 6 Rest, $-11 \equiv 18$ Nichtrest ist, so haben wir die Zeichenfolge $+ -$ zu nehmen, also die Kongruenzen

$6x^2 \equiv 16$	4	6	22	24	26	28
$18y^2 \equiv 2$	19	21	8	10	11	14

zu lösen, und diese liefern

$\pm x \equiv 14$	7	1	9	2	3	13
$\pm y \equiv 10$	14	8	9	6	12	2.

§. 127.

Matrots Bestimmung der Primzahlen, für welche $+2$ Rest ist.

Die Ergebnisse des §. 125 haben Matrot das Mittel gegeben, den in §. 116 und dann nochmals in §. 118 hergeleiteten Satz über die Primzahlen, von denen $+2$ quadratischer Rest oder Nichtrest ist, sehr einfach zu beweisen.

Wir nehmen an, der Modul sei eine ungerade Primzahl p , schreiben die Zahlen

$$(I) \quad 1, 2, 3, \dots, \frac{p-1}{2}, \frac{p+1}{2}, \dots, p-1$$

in eine Reihe und setzen unter jeden quadratischen Rest von p das Zeichen $+$, unter jeden Nichtrest das Zeichen $-$. Dann geht aus den in §. 125 erhaltenen Ausdrücken hervor, daß

$$R_n + N_r = \frac{p-1}{2}$$

ist, d. h., daß die Anzahl der Zeichenwechsel in der Reihe (I) $\frac{p-1}{2}$ beträgt. Außerdem leuchtet ein, daß in jedem Teil der Reihe das letzte und das erste Glied dasselbe Zeichen haben, wenn der Teil eine gerade Anzahl von Zeichenwechseln enthält, während eine ungerade Anzahl von Zeichenwechseln anzeigt, daß das Zeichen des ersten Gliedes des Teils demjenigen des letzten entgegengesetzt ist.

Wir führen nun die Untersuchung über den quadratischen Charakter von 2 auf denjenigen der Zahl $\frac{p+1}{2}$ zurück. Da nämlich

$$2 \cdot \frac{p+1}{2} = p+1 \equiv +1 \pmod{p},$$

also das Produkt der Zahlen 2 und $\frac{p+1}{2}$ ein Rest von p ist, so müssen nach §. 110 beide Zahlen entweder Reste sein, d. h. 2 ist Rest von p , wenn $\frac{p+1}{2}$ es ist, oder sie müssen beide Nichtreste sein, d. h. 2 ist Nichtrest von p , wenn $\frac{p+1}{2}$ es ist.

Nach diesen Vorbemerkungen schreiben wir die zweite Hälfte der Reihe (I) in umgekehrter Reihenfolge der Glieder unter die erste Hälfte:

$$(II) \quad 1, \quad 2, \quad 3, \quad \dots, \quad \frac{p-1}{2},$$

$$(III) \quad p-1, \quad p-2, \quad p-3, \quad \dots, \quad \frac{p+1}{2},$$

so daß je zwei unter einander stehende Glieder der erhaltenen Reihen (II) und (III) einander zum Modul ergänzen. Die Reihen (I), (II), (III) mögen beziehungsweise w_1, w_2, w_3 Zeichenwechsel enthalten. Da nun nach §. 115, Zusatz II die untereinander stehenden Glieder von (II) und (III) entweder sämtlich dieselben oder sämtlich entgegengesetzte Vorzeichen haben, so stimmen die Reihen (II) und (III) hinsichtlich der Zeichenwechsel vollständig überein, oder es ist $w_2 = w_3$. Die Zeichenwechsel von (II) und (III) finden sich sämtlich auch in (I) vor. Die letztere Reihe besitzt außerdem noch einen Zeichenwechsel, wenn die Zahlen

$$\frac{p-1}{2} \quad \text{und} \quad \frac{p+1}{2},$$

zwischen denen die Teilung von (I) in (II) und (III) erfolgte, verschiedene Zeichen haben, und da diese Zahlen einander zum Modul ergänzen, so ist das nur der Fall, wenn p die Form $4k+3$ hat. Es ist somit

$$\text{für } p = 4k+1 \quad w_2 = w_3 = \frac{1}{2} \quad w_1 = \frac{p-1}{4},$$

$$, \quad p = 4k+3 \quad w_2 = w_3 = \frac{1}{2} (w_1 - 1) = \frac{p-3}{4}.$$

Wir setzen erstens $p = 4k+1$ voraus. Wenn dann

$$w_2 = \frac{p-1}{4}$$

eine gerade Zahl $2n$ ist, so ergibt sich $p = 8n + 1$. In diesem Falle hat das letzte Glied von (II) denselben quadratischen Charakter wie das erste. Nun ist 1 Rest von p , folglich ist auch $\frac{p-1}{2}$ ein Rest. Dann muß aber auch $\frac{p+1}{2}$ und somit 2 ein Rest von $p = 8n + 1$ sein.

Wenn dagegen

$$w_2 = \frac{p-1}{4}$$

eine ungerade Zahl $2n + 1$ ist, so ergibt sich $p = 8n + 5$. In diesem Falle ist $\frac{p-1}{2}$ ein Nichtrest, da 1 ein Rest ist. Es ist dann $\frac{p+1}{2}$, somit auch 2 ein Nichtrest von $p = 8n + 5$.

Zweitens nehmen wir an, p habe die Form $4k + 3$. Wenn dann $w_2 = \frac{p-3}{4}$ eine gerade Zahl $2n$ ist, so ergibt sich $p = 8n + 3$.

In diesem Falle sind 1 und $\frac{p-1}{2}$ Reste, folglich $\frac{p+1}{2}$ und daher auch 2 ein Nichtrest von $p = 8n + 3$. Ist dagegen

$w_2 = \frac{p-3}{4}$ eine ungerade Zahl $2n + 1$, so ergibt sich $p = 8n + 7$.

In diesem Falle ist, da 1 ein Rest ist, $\frac{p-1}{2}$ ein Nichtrest, folglich $\frac{p+1}{2}$ und ebenso auch 2 ein Rest von $p = 8n + 7$.

§. 128.

Der Bachetsche Satz.

Jede Zahl, die nicht selbst eine Quadratzahl ist, kann als Summe von vier oder weniger Quadraten dargestellt werden¹⁾.

¹⁾ Bachet spricht den Satz in seinem Zusatz zu Diophants Arithmetik IV, 31 aus (vergl. die Übersetzung von Wertheim S. 162). Einen Beweis zu finden, ist weder ihm noch Euler gelungen. Erst Lagrange (Oeuvres III, p. 189) hat den von Diophant an verschiedenen Stellen stillschweigend vorausgesetzten Satz bewiesen. Eine Verallgemeinerung hat Fermat in seiner Ausgabe des Diophant gegeben (s. Wertheim, l. c.). Siehe auch Legendre, Théorie des Nombres I, p. 211 und Gauss, Disquisitiones 293.

Die von Euler (*Commentationes arithmeticae collectae* I, p. 543) gegebene Identität

$$\begin{aligned} & (a^2 + b^2 + c^2 + d^2)(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) \\ &= (a\alpha + b\beta + c\gamma + d\delta)^2 + (a\beta - b\alpha - c\delta + d\gamma)^2 \\ &+ (a\gamma + b\delta - c\alpha - d\beta)^2 + (a\delta - b\gamma + c\beta - d\alpha)^2 \end{aligned}$$

lehrt, daß der Satz von jeder zusammengesetzten Zahl gilt, sobald er für die einzelnen in derselben aufgehenden Primzahlen besteht. Wir können unsere Betrachtung also auf Primzahlen beschränken.

Hilfssatz. Jede Primzahl, welche in der Summe von vier Quadraten aufgeht, die prim zu einander sind, ist selbst die Summe von vier Quadraten.

Beweis (Lagrange, l. c.). Die Zahl p möge in der Summe

$$A^2 + B^2 + C^2 + D^2$$

aufgehen, und es seien A, B, C, D prim zu einander. Sind dann a, b, c, d beziehungsweise die absolut kleinsten Reste von A, B, C, D für den Modul p , also jede der Zahlen a, b, c, d dem absoluten Werte nach

$$< \frac{1}{2} p,$$

so geht p auch in

$$a^2 + b^2 + c^2 + d^2$$

auf, d. h. es ist

$$(1) \quad a^2 + b^2 + c^2 + d^2 = p p_1,$$

wo p_1 eine ganze Zahl bezeichnet. Da nun

$$a^2 + b^2 + c^2 + d^2 < 4 \cdot \left(\frac{1}{2} p\right)^2,$$

also $p p_1 < p^2$ ist, so muß $p_1 < p$ sein.

Wenn jetzt $p_1 = 1$ ist, so geht (1) über in

$$p = a^2 + b^2 + c^2 + d^2,$$

und dann ist der Satz bewiesen.

Wenn aber $p_1 > 1$ ist, so mögen a_1, b_1, c_1, d_1 beziehungsweise die absolut kleinsten Reste von a, b, c, d für den Modul p_1 bezeichnen; jede der Zahlen a_1, b_1, c_1, d_1 ist dann

$$< \frac{1}{2} p_1.$$

Da nun p_1 wegen (1) in

$$a^2 + b^2 + c^2 + d^2$$

aufgeht, so muß auch

$$a_1^2 + b_1^2 + c_1^2 + d_1^2$$

durch p_1 teilbar, etwa

$$(2) \quad a_1^2 + b_1^2 + c_1^2 + d_1^2 = p_1 p_2$$

sein, wo p_2 eine ganze Zahl bezeichnet, die, wie sich leicht beweisen läßt, $< p_1$ ist. Durch Multiplikation von (1) und (2) erhält man

$$(3) \quad \alpha^2 + \beta^2 + \gamma^2 + \delta^2 = p p_1^2 p_2,$$

wo nach der oben angegebenen Identität

$$(4) \quad \begin{cases} \alpha = a a_1 + b b_1 + c c_1 + d d_1 \\ \beta = a b_1 - b a_1 - c d_1 + d c_1 \\ \gamma = a c_1 + b d_1 - c a_1 - d b_1 \\ \delta = a d_1 - b c_1 + c b_1 - d a_1 \end{cases}$$

ist. Nun können a_1, b_1, c_1, d_1 als Reste von a, b, c, d für den Modul p_1 beziehungsweise durch

$$a - k_1 p_1, \quad b - k_2 p_1, \quad c - k_3 p_1, \quad d - k_4 p_1$$

ersetzt werden, wo k_1, k_2, k_3, k_4 ganze Zahlen bedeuten. Dann ergibt sich leicht

$$\begin{aligned} \alpha &= p_1 (p - a k_1 - b k_2 - c k_3 - d k_4), \\ \beta &= p_1 (-a k_2 + b k_1 + c k_4 - d k_3), \\ \gamma &= p_1 (-a k_3 - b k_4 + c k_1 + d k_2), \\ \delta &= p_1 (-a k_4 + b k_3 - c k_2 + d k_1). \end{aligned}$$

Da somit jede der Größen $\alpha, \beta, \gamma, \delta$ den Faktor p_1 enthält, so kann man die Gleichung (3) durch p_1^2 heben, und man erhält, wenn die ganzen Zahlen

$$\frac{\alpha}{p_1}, \quad \frac{\beta}{p_1}, \quad \frac{\gamma}{p_1}, \quad \frac{\delta}{p_1}$$

beziehungsweise mit a_2, b_2, c_2, d_2 bezeichnet werden,

$$(5) \quad a_2^2 + b_2^2 + c_2^2 + d_2^2 = p p_2.$$

Die Gleichung (5) hat dieselbe Form wie (1); es ist aber $p_2 < p_1$. Wenn jetzt $p_2 = 1$ ist, so ist p nach (5) die Summe von vier Quadraten. Ist dagegen $p_2 > 1$, so verfahren wir mit

(5), wie wir mit (1) verfahren haben; wir gelangen dadurch zu einer neuen Gleichung

$$(6) \quad a_3^2 + b_3^2 + c_3^2 + d_3^2 = p p_3,$$

wo $p_3 < p_2$ ist. Da die Zahlen $p, p_1, p_2, p_3, \dots$ eine abnehmende Reihe ganzer positiver Zahlen bilden, so muß endlich einmal ein $p_m = 1$ erscheinen, d. h. es muß sich

$$a_m^2 + b_m^2 + c_m^2 + d_m^2 = p$$

ergeben. p ist somit die Summe von vier Quadraten.

Anmerkung. Der Beweis verliert seine Geltung nicht, wenn man annimmt, daß eines oder zwei der vier Quadrate, welche $A^2 + B^2 + C^2 + D^2$ ausmachen, Null sind. Es kann auch vorkommen, daß eines oder zwei der vier Quadrate, welche den Divisor p ausmachen, Null sind. Es ist also jede Primzahl, welche in die Summe von vier oder weniger Quadraten aufgeht, wofern diese nur ohne gemeinschaftlichen Divisor sind, selbst die Summe von vier oder weniger Quadraten.

Lehrsatz. Jede Primzahl ist die Summe von vier oder weniger Quadraten.

I. Beweis. Wir betrachten die Kongruenz

$$x^2 + y^2 + 1 \equiv 0 \pmod{p}.$$

Da 1 ein Rest und -1 ein Rest oder ein Nichtrest von p ist, jenachdem p die Form $4n + 1$ oder $4n + 3$ hat, so hat die Kongruenz nach §. 126 jedesmal eine Lösung, wenn im ersteren Falle in der Reihe

$$1, 2, 3, \dots, p - 1$$

auf einen Rest ein Rest, im zweiten Falle auf einen Rest ein Nichtrest folgt. Nach §. 125 hat daher die Kongruenz, sobald $p > 5$ ist, immer wenigstens eine Lösung. Jede Primzahl, die > 5 ist, geht also in die Summe $x^2 + y^2 + 1$ auf und ist somit selbst die Summe von vier oder weniger Quadraten. Da nun noch der Satz auch für die Primzahlen $p \leq 5$ gilt, so gilt er allgemein.

II. Beweis (A. Matrot, Vortrag, gehalten am 9. August 1890 zu Limoges auf dem Kongress der Association française pour l'avancement des sciences).

Es sei $p = 2n + 1$ eine beliebige (ungerade) Primzahl, und es seien die Zahlen von 1 bis $p - 1$, mit Ausschluss von n und $2n$, in folgender Weise geordnet:

$$\begin{array}{c|c|c|c|c} 1 & 2 & 3 & \dots & n-1 \\ 2n-1 & 2n-2 & 2n-3 & \dots & n+1 \end{array}$$

Zwei untereinander stehende Zahlen, die ein Paar heißen sollen, haben also die Summe $2n$. Nun befinden sich unter den Zahlen von 1 bis $p - 1$ bekanntlich

$$\frac{1}{2}(p-1) = n$$

quadratische Reste von p , und da nur $n - 1$ Paare niedergeschrieben sind, so müssen entweder beide Zahlen wenigstens eines Paares Reste sein, oder es muß wenigstens eine der nicht hingeschriebenen Zahlen (n und $2n$) ein Rest sein.

Es seien erstens α, α' die Zahlen eines Paares, welche beide Reste von p sind. Dann giebt es zwei ganze Zahlen a, a' , für welche

$$a^2 \equiv \alpha, \quad a'^2 \equiv \alpha',$$

also

$$a^2 + a'^2 \equiv \alpha + \alpha' \equiv 2n \equiv p - 1 \equiv -1 \pmod{p},$$

oder

$$a^2 + a'^2 + 1$$

durch p teilbar ist.

Zweitens sei n ein quadratischer Rest von p ; dann giebt es eine Zahl a , für welche

$$a^2 \equiv n, \quad \text{also} \quad 2a^2 \equiv 2n,$$

d. i.

$$2a^2 \equiv p - 1 \equiv -1 \pmod{p}$$

ist. In diesem Falle ist also $a^2 + a^2 + 1$ durch p teilbar.

Wenn endlich $2n = p - 1$ Rest von p ist, so giebt es eine Zahl a , für welche

$$a^2 \equiv p - 1 \equiv -1 \pmod{p},$$

also $a^2 + 1$ durch p teilbar ist.

Somit geht jede ungerade Primzahl in die Summe von drei oder weniger Quadraten auf, welche prim zu einander sind. Jede Primzahl läßt sich also in vier oder weniger Quadrate zerfallen.

§. 129.

Aufgaben.

I. Die Kongruenz

$$x^2 \equiv 365 \pmod{1847}$$

zu lösen.

Es ist

$$x \equiv \pm 365^{462} \equiv \pm 496 \pmod{1847}.$$

$$[365^2 \equiv 241, 365^4 \equiv 824, 365^8 \equiv -720, 365^{16} \equiv -607, \\ 365^{32} \equiv -951, 365^{64} \equiv -629, 365^{128} \equiv 383, 365^{256} \equiv 776, \\ 365^{512} \equiv -159, 365^{1024} \equiv 273, 365^{2048} \equiv -778, 365^{4096} \equiv -163, \\ 365^{8192} \equiv -496.]$$

II.

$$1) \quad x^2 \equiv 35 \pmod{437 = 19 \cdot 23}.$$

$$[x \equiv \pm 129, \pm 175 \pmod{437}.]$$

$$2) \quad x^2 \equiv 9 \pmod{27}.$$

$$[x \equiv \pm 3, \pm 12, \pm 21 \pmod{27}.]$$

$$3) \quad x^2 \equiv 25 \pmod{75}.$$

$$[\pm x = 5, 20, 35, 50, 65 \pmod{75}.]$$

III. Die Kongruenz $x^2 \equiv 75 \pmod{179}$ hat die Wurzeln ± 84 . Welches sind die Wurzeln der Kongruenz

$$x^2 \equiv 3 \pmod{179}? [x \equiv \pm 19 \pmod{179},$$

denn aus

$$5\xi \equiv 84 \equiv -95$$

folgt

$$\xi \equiv -19 \pmod{179}].$$

IV. Ist die Kongruenz $x^2 \equiv 750 \pmod{947}$ möglich oder nicht?

$$\left(\frac{750}{947}\right) = \left(\frac{25 \cdot 30}{947}\right) = \left(\frac{30}{947}\right) = \left(\frac{2}{947}\right) \left(\frac{3}{947}\right) \left(\frac{5}{947}\right) = +1,$$

denn

$$\left(\frac{2}{947}\right) = -1, \text{ weil } 947 \text{ von der Form } 8n + 3 \text{ ist,}$$

$$\left(\frac{3}{947}\right) = +1, \text{ weil } 947 \text{ von der Form } 12n + 11 \text{ ist,}$$

$$\left(\frac{5}{947}\right) = -1, \text{ weil } \left(\frac{5}{947}\right) = \left(\frac{947}{5}\right) = \left(\frac{2}{5}\right) \text{ ist.}$$

Die Kongruenz ist also möglich; ihre Wurzeln sind

$$x \equiv 750^{237} \equiv \pm 312 \pmod{947}.$$

V. Alle Lösungen der Kongruenz

$$13x^2 + 3y^2 \equiv 11 \pmod{29}$$

zu finden.

$\pm x$	0	14	7	1	9	2	3	13
$\pm y$	9	11	2	3	7	5	10	8

VI. Die Zahl $7043 = 84^2 - 13$ unter Anwendung der Formen der Divisoren von $x^2 - 13$ in Faktoren zu zerlegen.

Die Zahl 7043 ist eine Primzahl, da keine der Primzahlen

3, 17, 23, 29, 43, 53, 61, 79

in sie aufgeht.

$$\text{Desgl. } 8483 = 92^2 + 19 \quad [17.499].$$

$$,, \quad 9197 = 96^2 - 19 \quad [17.541].$$

$$,, \quad 8083 = 90^2 - 17 \quad [59.137].$$

VII. Die Zahl 2972191 in Faktoren zu zerlegen.

Es ist

$$\sqrt{2972191} = 1724^2 + 15.$$

Die Formen der Divisoren von $x^2 + 15$ (S. 377) enthalten die Primzahlen

61, 79, 83, 107, 109, 113, 137, 139, 151, 167, 173, 181, 197, 199, 211, 227, 229, 233, ...

Die kleinste in die vorgelegte Zahl aufgehende dieser Primzahlen ist 229, und man erhält

$$2972191 = 229 \cdot 12979.$$

VIII. Die Zahl $2^{25} - 1 = 33554431$ in Faktoren zu zerlegen (Legendre, Théorie des Nombres I, p. 334).

Bekanntlich ist $2^{25} - 1$ durch $2^5 - 1 = 31$ teilbar; die Division ergibt den Quotienten 1082401, der nicht durch 31 teilbar ist. Nun muß jede andere in $2^{25} - 1$ aufgehende ungerade Primzahl p von der Form $50k + 1$ sein. Da sie aber auch in $2(2^{25} - 1) = 2^{26} - 2$ aufgehen muß, so gehört sie zu den Primzahlen, für welche die Kongruenz $x^2 \equiv 2$ möglich, also 2 quadratischer Rest ist. p befindet sich daher unter den Prim-

zahlen der beiden Formen $8n \pm 1$. Vereinigt man nach §. 38 die beiden Bedingungen, denen p unterliegt, so ergibt sich, daß die Zahl p unter den Primzahlen der beiden Formen

$$200k + 1, \quad 200k + 151$$

zu suchen ist. Außerdem kommen nur die Primzahlen in Betracht, welche kleiner als $\sqrt{1082401}$ sind, d. i. unterhalb 1040 liegen. Es sind das nur die vier Zahlen 151, 401, 601, 751. Die dritte derselben geht auf, und man erhält auf diese Weise

$$2^{25} - 1 = 31.601.1801.$$

IX. Es soll bewiesen werden, daß $ax^2 \pm b$ keinen Divisor hat, der nicht auch ein Divisor von $x^2 \pm ab$ wäre.

Wenn $ax^2 \pm b$ für den Wert $x = \xi$ durch die Primzahl p teilbar ist, so geht p auch in $a(a\xi^2 \pm b) = (a\xi)^2 \pm ab$ auf $x^2 \pm ab$ ist also für den Wert $x = a\xi$ durch p teilbar.

Z u s ä t z e.

Zu S. 17. Jedem ungeraden Divisor $d = 2\delta + 1$ einer Zahl $N = dn$ entspricht eine Darstellung von N als Summe aufeinander folgender Zahlen. Die Zahl N selbst wird dabei ebenfalls als eine Zerlegung angesehen, und zwar entspricht sie dem Divisor $d = 1$. Es ist nämlich

$$N = (n - \delta) + (n - \delta + 1) + \dots + n + \dots + (n + \delta).$$

Die Anzahl der Zerlegungen ist also gleich der Anzahl der ungeraden Divisoren (Sylvester, Comptes rendus 96).

Beispiele.

I. $N = 30$.

Ungerader Divisor	Entsprechende Zerlegung
1	30
3	9 + 10 + 11
5	4 + 5 + 6 + 7 + 8
15	6 + 7 + 8 + 9.

II. $N = 45$.

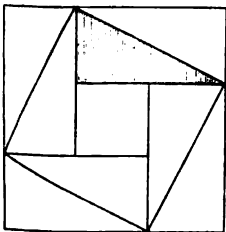
Ungerader Divisor	Entsprechende Zerlegung
1	45
3	14 + 15 + 16
5	7 + 8 + 9 + 10 + 11
9	1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9
15	5 + 6 + 7 + 8 + 9 + 10
45	22 + 23.

Zu S. 49. Für einige Werte von m sind die $\varphi(m)$ Zahlen, die prim zu m und nicht größer als m sind, sämtlich Primzahlen, wofür auch 1 zu den Primzahlen gerechnet wird. Damit eine Zahl m diese Eigenschaft habe, muß sie offenbar durch sämtliche Primzahlen teilbar sein, die $\leq \sqrt{m}$ sind. Von dieser Beschaffenheit sind die Zahlen

$$m = 1, 2, 3, 4, 6, 8, 12, 18, 24, 30.$$

Dafs es über 30 hinaus keine solche Zahl mehr giebt, ist von E. Landau bewiesen [Archiv der Math. u. Phys. III. Reihe, B. 1 (1901), S. 138].

Zu S. 64. Man erhält die Lösung der S. 64 erwähnten und S. 147 behandelten Aufgabe unmittelbar durch den in der nebenstehenden Figur veranschaulichten, von Diophant mehrmals, z. B. III, 22, ebenso V, 9 u. s. w. ausgesprochenen Satz: „Das Quadrat über der Hypotenuse eines rechtwinkligen Dreiecks bleibt ein Quadrat sowohl bei Addition, als auch bei Subtraktion des vierfachen Flächeninhalts des Dreiecks.“ Sind nämlich



$$m^2 + n^2, \quad m^2 - n^2, \quad 2mn$$

die Seiten des Dreiecks, so ist

$$(m^2 + n^2)^2 + 4mn(m^2 - n^2) = (m^2 - n^2 + 2mn)^2,$$

$$(m^2 + n^2)^2 - 4mn(m^2 - n^2) = (m^2 - n^2 - 2mn)^2.$$

Zu S. 140. Die von Euler bewiesene Unmöglichkeit einer rationalen Lösung der Gleichung $x^3 + y^3 = z^3$ war schon den Arabern bekannt. Siehe die „Essenz der Rechenkunst von

Mohammed Beha-eddin Alhossain“, arabisch und deutsch herausgegeben von G. H. F. Nesselmann (Berlin 1843), S. 56.

Zu S. 220. Die unrichtige Benennung „Pellische Gleichung“ rührt von Euler her. Siehe meine Bemerkungen in den „Abhandlungen zur Geschichte der Mathematik“ IX, S. 562 und in der Bibliotheca mathematica 3. Folge I, S. 360; III, S. 113; ebenso Eneström, ebenda III, S. 204.

Zu S. 258. Der in §. 84 bewiesene Satz von Epstein gilt auch, wenn der Modul m eine Potenz einer ungeraden Primzahl oder das Doppelte einer solchen Potenz ist. Es läßt sich nämlich wie im Falle eines Primzahlmoduls beweisen, daß, wenn g eine primitive Wurzel von m und k prim zu $\varphi(m)$ ist, auch g^k eine primitive Wurzel von m sein wird, daß unter dieser Voraussetzung ferner, da dann $\varphi(m) - k$ prim zu $\varphi(m)$ ist, auch $g^{\varphi(m)-k}$ eine primitive Wurzel von g ist, und daß endlich, da

$$g^k \cdot g^{\varphi(m)-k} = g^{\varphi(m)} \equiv 1 \pmod{m}$$

ist, sich die $\varphi(m)$ primitiven Wurzeln von m in der Weise zu je zweien zusammenstellen lassen, daß das Produkt der beiden Wurzeln jedes Paares für den Modul m den Rest 1 liefert.

Da nun die für zwei primitive Wurzeln g, g_1 , für welche

$$g \cdot g_1 \equiv 1 \pmod{m}$$

ist, genommenen kleinsten Indizes α, α_1 einer jeden Zahl a der Bedingung

$$\alpha + \alpha_1 = \varphi(m)$$

genügen, so ist die Summe aller kleinsten Indizes von a

$$\frac{1}{2} \varphi(m) \cdot \varphi(m).$$

Beispiel. Es sei $m = 49$. Die Zahl 4 hat für die

primitive Wurzel.	3	33	5	10	12	45	17	26	24	47	38	40
den Index	10	32	38	4	20	22	34	8	40	2	16	26.

Ebenso gilt der Satz für den Modul 2^x , wenn $x > 3$ ist. Nimmt man für jede der 2^{x-3} Zahlen der Form

$$8n + 3 \text{ [resp. } 8n + 5]$$

als Basis den kleinsten Index einer der 2^{x-3} Zahlen der beiden Formen

$$8n + 3, \quad 8n + 1 \text{ [resp. } 8n + 5, \quad 8n + 1],$$

so ist die Summe der Indizes 2^{x-1} . Eine Ausnahme macht natürlich in allen Fällen die Zahl 1, welche im Falle eines Primzahlmoduls p den Index $p - 1$, für die Moduln $m = p^2$ und $2p^2$ den Index

$$\varphi(m) = (p - 1)p^{2-1}$$

und für den Modul 2^x den Index 2^{x-2} hat, für welche also die Summe der Indizes stets doppelt so viel wie für jede andere Zahl beträgt.

Beispiel. Für den Modul $2^5 = 32$ erhält man leicht die Tabelle:

Basis	Z a h l e n							
	1	3	9	11	17	19	25	27
	I n d i z e s							
3	8	1	2	7	4	5	6	3
11	8	7	6	1	4	3	2	5
19	8	5	2	3	4	1	6	7
27	8	3	6	5	4	7	2	1.

Anhang

enthaltend:

1. Die Tabelle der Primzahlen unter 10000 mit Angabe der kleinsten primitiven Wurzeln für alle unter 6200 und für einige zwischen 6200 und 10000 liegende Primzahlen.
 2. Die Wurzeln der Kongruenz $ax \equiv 1 \pmod{p}$ für alle unter 100 liegenden Primzahlen p und a .
 3. Indizes-Tafeln für das Zahlengebiet von 1 bis 100.
 4. Die kleinste Lösung der Gleichung $x^2 - ay^2 = \pm 1$ für die unter 100 liegenden Werte von a .
 5. Die Formen der Divisoren von $x^2 \pm a$ für die Werte von $a = 1$ bis $a = 23$.
 6. Eine graphische Darstellung des Reziprozitätssatzes für alle Primzahlen unter 100.
-

I. Tabelle

der ungeraden Primzahlen unter 10000. Für alle bis 6200 und für einige darüber hinaus liegenden Primzahlen p ist die kleinste primitive Wurzel g hinzugefügt. Auch ist jede Primzahl, für welche 10 eine primitive Wurzel ist, mit dem Zeichen * versehen.

p	g	p	g	p	g	p	g	p	g
3	2	181*	2	421	2	673	5	953*	3
5	2	191	19	431	7	677	2	967	5
7*	3	193*	5	433*	5	683	5	971*	6
11	2	197	2	439	15	691	3	977*	3
13	2	199	3	443	2	701*	2	983*	5
17*	3	211	2	449	3	709*	2	991	6
19*	2	223*	3	457	13	719	11	997	7
23*	5	227	2	461*	2	727*	5	1009	11
29*	2	229*	6	463	3	733	6	1013	3
31	3	233*	3	467	2	739	3	1019*	2
37	2	239	7	479	13	743*	5	1021*	10
41	6	241	7	487*	3	751	3	1031	14
43	3	251	6	491*	2	757	2	1033*	5
47*	5	257*	3	499*	7	761	6	1039	3
53	2	263*	5	503*	5	769	11	1049	3
59*	2	269*	2	509*	2	773	2	1051*	7
61*	2	271	6	521	3	787	2	1061	2
67	2	277	5	523	2	797	2	1063*	3
71	7	281	3	541*	2	809	3	1069*	6
73	5	283	3	547	2	811*	3	1087*	3
79	3	293	2	557	2	821*	2	1091*	2
83	2	307	5	563	2	823*	3	1093	5
89	3	311	17	569	3	827	2	1097*	3
97*	5	313*	10	571*	3	829	2	1103*	5
101	2	317	2	577*	5	839	11	1109*	2
103	5	331	3	587	2	853	2	1117	2
107	2	337*	10	593*	3	857*	3	1123	2
109*	6	347	2	599	7	859	2	1129	11
113*	3	349	2	601	7	863*	5	1151	17
127	3	353	3	607	3	877	2	1153*	5
131*	2	359	7	613	2	881	3	1163	5
137	3	367*	6	617	3	883	2	1171*	2
139	2	373	2	619*	2	887*	5	1181*	7
149*	2	379*	2	631	3	907	2	1187	2
151	6	383*	5	641	3	911	17	1193*	3
157	5	389*	2	643	11	919	7	1201	11
163	2	397	5	647*	5	929	3	1213	2
167*	5	401	3	653	2	937*	5	1217*	3
173	2	409	21	659*	2	941*	2	1223*	5
179*	2	419*	2	661	2	947	2	1229*	2

<i>p</i>	<i>g</i>	<i>p</i>	<i>g</i>	<i>p</i>	<i>g</i>	<i>p</i>	<i>g</i>	<i>p</i>	<i>g</i>
1231	3	1601	3	1997	2	2377	5	2753*	3
1237	2	1607*	5	1999	3	2381	3	2767*	3
1249	7	1609	7	2003	5	2383*	5	2777*	3
1259*	2	1613	3	2011	3	2389*	2	2789*	2
1277	2	1619*	2	2017*	5	2393	3	2791	6
1279	3	1621*	2	2027	2	2399	11	2797	2
1283	2	1627	3	2029*	2	2411*	6	2801	3
1289	6	1637	2	2039	7	2417*	3	2803	2
1291*	2	1657	11	2053	2	2423*	5	2819*	2
1297*	10	1663*	3	2063*	5	2437	2	2833*	5
1301*	2	1667	2	2069*	2	2441	6	2837	2
1303*	6	1669	2	2081	3	2447*	5	2843	2
1307	2	1693	2	2083	2	2459*	2	2851*	2
1319	13	1697*	3	2087	5	2467	2	2857	11
1321	13	1699	3	2089	7	2473*	5	2861*	2
1327*	3	1709*	3	2099*	2	2477	2	2879	7
1361	3	1721	3	2111	7	2503	3	2887*	5
1367*	5	1723	3	2113*	5	2521	17	2897*	3
1373	2	1733	2	2129	3	2531	2	2903*	5
1381*	2	1741*	2	2131	2	2539*	2	2909*	2
1399	13	1747	2	2137*	10	2543*	5	2917	5
1409	3	1753	7	2141*	2	2549*	2	2927*	5
1423	3	1759	6	2143*	3	2551	6	2939*	2
1427	2	1777*	5	2153*	3	2557	2	2953	13
1429*	6	1783*	10	2161	14	2579*	2	2957	2
1433*	3	1787	2	2179*	7	2591	7	2963	2
1439	7	1789*	6	2203	5	2593*	7	2969	3
1447*	3	1801	11	2207*	5	2609	3	2971*	10
1451	2	1811*	6	2213	2	2617*	5	2999	17
1453	2	1823*	5	2221*	2	2621*	2	3001	14
1459	3	1831	3	2237	2	2633*	3	3011*	2
1471	6	1847*	5	2239	3	2647	3	3019*	2
1481	3	1861*	2	2243	2	2657*	3	3023*	5
1483	2	1867	2	2251*	7	2659	2	3037	2
1487*	5	1871	14	2267	2	2663*	5	3041	3
1489	14	1873*	10	2269*	2	2671	7	3049	11
1493	2	1877	2	2273*	3	2677	2	3061	6
1499	2	1879	6	2281	7	2683	2	3067	2
1511	11	1889	3	2287	19	2687*	5	3079	6
1523	2	1901	2	2293	2	2689	19	3083	2
1531*	2	1907	2	2297*	5	2693	2	3089	3
1543*	5	1913*	3	2309*	2	2699*	2	3109	6
1549*	2	1931	2	2311	3	2707	2	3119	7
1553*	3	1933	5	2333	2	2711	7	3121	7
1559	19	1949*	2	2339*	2	2713*	5	3137*	3
1567*	3	1951	3	2341*	7	2719	3	3163	3
1571*	2	1973	2	2347	3	2729	3	3167*	5
1579*	3	1979*	2	2351	13	2731*	3	3169	7
1583*	5	1987	2	2357	2	2741*	2	3181	7
1597	11	1993	5	2371*	2	2749	6	3187	2

408 Primzahlen mit ihren kleinsten primitiven Wurzeln.

<i>p</i>	<i>g</i>	<i>p</i>	<i>g</i>	<i>p</i>	<i>g</i>	<i>p</i>	<i>g</i>	<i>p</i>	<i>g</i>
3191	11	3583	3	4003	2	4423*	3	4871	11
3203	2	3593*	3	4007*	5	4441	21	4877	2
3209	3	3607*	5	4013	2	4447*	3	4889	3
3217	5	3613	2	4019*	2	4451*	2	4903	3
3221*	10	3617*	3	4021	2	4457*	3	4909	6
3229	6	3623*	5	4027	3	4463*	5	4919	13
3251*	6	3631	21	4049	3	4481	3	4931*	6
3253	2	3637	2	4051*	10	4483	2	4933	2
3257*	3	3643	2	4057*	5	4493	2	4937*	3
3259*	3	3659*	2	4073*	3	4507	2	4943*	7
3271	3	3671	13	4079	11	4513	7	4951	6
3299*	2	3673*	5	4091*	2	4517	2	4957	2
3301*	6	3677	2	4093	2	4519	3	4967*	5
3307	2	3691	2	4099*	2	4523	5	4969	11
3313*	10	3697	5	4111	17	4547	2	4973	2
3319	6	3701*	2	4127*	5	4549	6	4987	2
3323	2	3709*	2	4129	13	4561	11	4993	5
3329	3	3719	7	4133	2	4567*	3	4999	3
3331*	3	3727*	3	4139*	2	4583*	5	5003	2
3343*	5	3733	2	4153*	5	4591	11	5009	3
3347	2	3739	7	4157	2	4597	5	5011	2
3359	11	3761	3	4159	3	4603	2	5021*	3
3361	22	3767*	5	4177*	5	4621	2	5023	3
3371*	2	3769	7	4201	11	4637	2	5039	11
3373	5	3779*	2	4211*	6	4639	3	5051	2
3389*	3	3793	5	4217*	3	4643	5	5059*	2
3391	3	3797	2	4219*	2	4649	3	5077	2
3407*	5	3803	2	4229*	2	4651*	3	5081	3
3413	2	3821*	3	4231	3	4657	15	5087*	5
3433*	5	3823	3	4241	3	4663	3	5099*	2
3449	3	3833*	3	4243	2	4673*	3	5101	6
3457	7	3847*	5	4253	2	4679	11	5107	2
3461*	2	3851	2	4259*	2	4691*	2	5113	19
3463*	3	3853	2	4261*	2	4703*	5	5119	3
3467	2	3863*	5	4271	7	4721	6	5147	2
3469*	2	3877	2	4273	5	4723	2	5153*	5
3491	2	3881	13	4283	2	4729	17	5167*	6
3499	2	3889	11	4289	3	4733	5	5171	2
3511	7	3907	2	4297	5	4751	19	5179*	2
3517	2	3911	13	4327*	3	4759	3	5189*	2
3527*	5	3917	2	4337*	3	4783*	6	5197	7
3529	17	3919	3	4339*	10	4787	2	5209	17
3533	2	3923	2	4349*	2	4789	2	5227	2
3539*	2	3929	3	4357	2	4793*	3	5231	7
3541	7	3931	2	4363	2	4799	7	5233*	10
3547	2	3943*	3	4373	2	4801	7	5237	3
3557	2	3947	2	4391	14	4813	2	5261	2
3559	3	3967*	6	4397	2	4817*	3	5273*	3
3571*	2	3989*	2	4409	3	4831	3	5279	7
3581*	2	4001	3	4421*	3	4861	11	5281	7

<i>p</i>	<i>g</i>	<i>p</i>	<i>g</i>	<i>p</i>	<i>g</i>	<i>p</i>	<i>g</i>	<i>p</i>	<i>g</i>
5297*	3	5711	29	6151	3	6581		7013	2
5303*	5	5717	2	6163	3	6599	13	7019*	
5309*	2	5737*	5	6173	2	6607		7027	
5323	5	5741*	2	6197	2	6619*		7039	
5333	2	5743*	10	6199	3	6637		7043	
5347	3	5749*	2	6203	2	6653	2	7057*	
5351	11	5779*	2	6211*	2	6659*	2	7069*	
5381*	3	5783*	7	6217*	5	6661*		7079	7
5387	2	5791	6	6221*	3	6673*		7103*	
5393*	3	5801	3	6229	2	6679		7109*	2
5399	7	5807*	5	6247*		6689		7121	
5407	3	5813	2	6257*		6691*		7127	
5413	5	5821*	6	6263*		6701*		7129	
5417*	3	5827	2	6269*	2	6703*		7151	
5419*	3	5839	6	6271		6709*		7159	
5431	3	5843	2	6277		6719	11	7177*	
5437	5	5849	3	6287*	7	6733		7187	2
5441	3	5851	2	6299		6737*	3	7193*	
5443	2	5857*	7	6301*	10	6761		7207*	3
5449	7	5861*	3	6311	7	6763		7211	
5471	7	5867	5	6317	2	6779*	2	7213	
5477	2	5869*	2	6323		6781		7219*	
5479	3	5879	11	6329		6791		7229*	
5483	2	5881	31	6337*		6793*		7237	
5501*	2	5897*	3	6343*		6803		7243	
5503*	3	5903*	5	6353*	3	6823*		7247*	5
5507	2	5923	2	6359		6827	2	7253	
5519	13	5927*	5	6361		6829*		7283	
5521	11	5939*	2	6367*		6833*		7297	
5527*	5	5953	7	6373		6841		7307	
5531*	10	5961*	3	6379		6857*	3	7309*	
5557	2	5987	2	6389*	2	6863*		7321	
5563	2	6007	3	6397		6869*		7331	
5569	13	6011*	2	6421		6871		7333	
5573	2	6029*	2	6427		6883		7349*	
5581*	6	6037	5	6449		6899*	2	7351	
5591	11	6043	5	6451		6907	2	7369	
5623*	5	6047*	5	6469		6911		7393*	
5639	7	6053	2	6473*	3	6917		7411*	
5641	14	6067	2	6481		6947		7417	
5647	3	6073*	10	6491		6949*		7433*	3
5651*	2	6079	17	6521		6959		7451*	
5653	5	6089	3	6529		6961		7457*	3
5657*	3	6091	7	6547		6967*		7459*	
5659*	2	6101	2	6551		6971*		7477	
5669*	3	6113*	3	6553*		6977*	3	7481	
5683	2	6121	7	6563	5	6983*	5	7487*	
5689	11	6131*	2	6569	3	6991		7489	
5693	2	6133	5	6571*		6997		7499*	
5701*	2	6143*	5	6577		7001		7507	

410 Primzahlen mit ihren kleinsten primitiven Wurzeln.

<i>p</i>	<i>g</i>	<i>p</i>	<i>g</i>	<i>p</i>	<i>g</i>	<i>p</i>	<i>g</i>	<i>p</i>	<i>g</i>
7517	2	7983		8419		8839		9311	
7523	2	7937*	3	8423*	5	8849		9319	
7529	3	7949*	2	8429*		8861*		9323	
7537		7951		8431		8863*		9337	
7541*		7963		8443		8867		9341*	
7547		7993		8447*		8887*		9343*	
7549		8009		8461		8893		9349	
7559	13	8011		8467		8923	2	9371*	
7561		8017*		8501*		8929		9377*	3
7573		8039	11	8513*		8933		9391	
7577*	3	8053		8521		8941		9397	
7583*		8059*		8527		8951		9403	
7589		8069*	2	8537*		8963	2	9413	
7591		8081		8539		8969		9419	
7603		8087*		8543*	5	8971*		9421*	
7607*	5	8089		8563		8999		9431	
7621		8093		8573	2	9001		9433	
7639		8101	6	8581		9007		9437	
7643	2	8111		8597		9011*		9439	
7649	3	8117	2	8599		9013		9461*	
7669		8123		8609	3	9029*		9463	
7673*		8147	2	8623*		9041		9467	2
7681	17	8161		8627		9043		9473*	3
7687*		8167		8629		9049		9479	
7691*		8171*		8641		9059*		9491*	
7699*		8179*		8647*		9067		9497*	3
7703*	5	8191		8663*		9091		9511	
7717		8209		8669*		9103*		9521	
7723		8219*		8677		9109*		9533	2
7727*	5	8221		8681		9127		9589*	2
7741		8231		8699		9133		9547	
7753*		8233*		8693		9137*	3	9551	
7757		8237		8699*	2	9151		9587	2
7759		8243		8707		9157		9601	
7789		8263*		8713*		9161		9613	
7793*	3	8269*		8719		9173	2	9619	
7817*	3	8273*		8731*		9181		9623*	5
7823*	5	8287*		8737		9187		9629*	
7829*		8291*		8741*		9199		9631	
7841		8293		8747	2	9203		9643	
7853		8297*		8753*	3	9209	3	9649	
7867		8311		8761		9221*		9661	
7873*		8317		8779		9227		9677	
7877		8329		8783*	5	9239		9679	
7879		8353*		8803		9241		9689	
7883		8363		8807*		9257*		9697*	
7901*		8369	3	8819*	2	9277		9719	
7907		8377*		8821*		9281		9721	
7919		8387		8831		9283		9733	
7927*		8389*		8837	2	9293		9739*	

p	g	p	g	p	g	p	g	p	g
9743*	5	9791		9839	7	9887*	5	9941	
9749*	2	9803		9851*		9901	2	9949*	
9767*		9811*		9857*		9907		9967*	
9769		9817*		9859		9923		9973	
9781*		9829*		9871		9929			
9787		9833*	3	9883		9931*			

II. Die Wurzeln der Kongruenz $ax \equiv 1 \pmod{p}$
für alle unterhalb 100 liegenden Primzahlen p und a .

p																								
3 5 7 11 13					17 19 23 29 31					37 41 43 47 53					59 61 67 71 73					79 83 89 97				
a									x												a			
2	2	3	4	6 7	9	10	12	15	16	19	21	22	24	27	30	31	34	36	37	40	42	45	49	2
3	2	5	4	9	6	13	8	10	21	25	14	29	16	18	20	41	45	24	49	53	28	30	65	3
5	3	9	8		7	4	14	6	25	15	33	26	19	32	12	49	27	57	44	16	50	18	39	5
7	8	2			5	11	10	25	9	16	6	37	27	38	17	35	48	61	21	34	12	51	14	7
11	6				14	7	21	8	17	27	15	4	30	29	43	50	61	13	20	36	68	81	53	11
13					4	3	16	9	12	20	19	10	29	49	50	47	31	11	45	73	32	48	15	13
17					9	19	12	11		24	29	38	36	25	7	18	4	46	43	14	44	21	40	17
19					17	26	18			2	13	34	5	14	28	45	60	15	50	25	35	75	46	19
23					24	27				29	25	15	45	30	18	8	35	34	54	55	65	31	38	23
29					15					23	17	3	13	11	57	40	37	49	68	30	63	43	87	29
31										6	4	25	44	12	40	2	13	55	33	51	75	23	72	31
37										10	7	14	43		8	33	29	48	2	47	9	77	21	37
41										21	39	22			36	3	18	26	57	27	81	76	71	41
43										35	37				11	44	53	38	17	68	56	29	88	43
47										44					54	13	10	68	14	37	53	36	64	47
53															49	38	43	67	62	3	47	42	11	53
59															30	25	65	26		75	38	86	74	59
61															11	7	6			57	49	54	35	61
67															53	12				46	57	4	42	67
71															36					69	76	84	41	71
73																				13	58	50	4	73
79																				62	80	70		79
83																				74	90			83
89																					12			89

Wenn der Koeffizient von x die m^{te} Potenz einer Primzahl a ist, so wird die dem Werte a entsprechende Lösung auf die m^{te} Potenz erhoben.

Wenn der Koeffizient von x ein Produkt ist, so werden die den einzelnen Faktoren entsprechenden Lösungen multipliziert.

Wenn die rechte Seite der Kongruenz nicht 1, sondern b ist, so wird die dem Werte 1 entsprechende Lösung mit b multipliziert.

Die vorstehende Tabelle giebt also die Lösung jeder Kongruenz ersten Grades, deren Modul eine Primzahl unter 100 ist.

Modul	Basis	Zahlen															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3	2	2	1														
4	3	2	—	1													
5	2	4	1	3	2												
6	5	2	—	—	—	1											
7	3	6	2	1	4	5	3										
8	3	2	—	1	—	—	—	—									
9	2	6	1	—	2	5	—	4	3								
10	3	4	—	1	—	—	—	3	—	2							
11	2	10	1	8	2	4	9	7	3	6	5						
13	2	12	1	4	2	9	5	11	3	8	10	7	6				
14	3	6	—	1	—	5	—	—	—	2	—	4	—	3			
16	3	4	—	1	—	—	—	—	—	2	—	3	—	—	—		
17	3	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8
18	5	6	—	—	—	1	—	2	—	—	—	5	—	4	—	—	—
19	2	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4
22	7	10	—	4	—	2	—	1	—	8	—	—	—	3	—	6	—
23	5	22	2	16	4	1	18	19	6	10	3	9	20	14	21	17	8
25	2	20	1	7	2	—	8	5	3	14	—	16	9	19	6	—	4
26	7	12	—	8	—	3	—	1	—	4	—	5	—	—	—	11	—
27	2	18	1	—	2	5	—	16	3	—	6	13	—	8	17	—	4
29	2	28	1	5	2	22	6	12	3	10	23	25	7	18	13	27	4
31	3	30	24	1	18	20	25	28	12	2	14	23	19	11	22	21	6
32	3	8	—	1	—	—	—	—	—	2	—	7	—	—	—	—	—
34	3	16	—	1	—	5	—	11	—	2	—	7	—	4	—	6	—
37	2	36	1	26	2	23	27	32	3	16	24	30	28	11	33	13	4
38	3	18	—	1	—	4	—	6	—	2	—	12	—	17	—	5	—
41	6	40	26	15	12	22	1	39	38	30	8	3	27	31	25	37	24
43	3	42	27	1	12	25	28	35	39	2	10	30	13	32	20	26	24
46	5	22	—	16	—	1	—	19	—	10	—	9	—	14	—	17	—
47	5	46	18	20	36	1	38	32	8	40	19	7	10	11	4	21	26
49	3	42	26	1	10	29	27	—	36	2	13	40	11	33	—	30	20
50	3	20	—	1	—	—	—	15	—	2	—	8	—	17	—	—	—
53	2	52	1	17	2	47	18	14	3	34	48	6	19	24	15	12	4
54	5	18	—	—	—	1	—	14	—	—	—	17	—	16	—	—	—
58	3	28	—	1	—	10	—	8	—	2	—	5	—	26	—	11	—
59	2	58	1	50	2	6	51	18	3	42	7	25	52	45	19	56	4
61	2	60	1	6	2	22	7	49	3	12	23	15	8	40	50	28	4
62	3	30	—	1	—	20	—	28	—	2	—	23	—	11	—	21	—
64	3	16	—	1	—	—	—	—	—	2	—	7	—	—	—	—	—
67	2	66	1	39	2	15	40	23	3	12	16	59	41	19	24	54	4
71	7	70	6	26	12	28	32	1	18	52	34	31	38	39	7	54	24
73	5	72	8	6	16	1	14	33	24	12	9	55	22	59	41	7	32
74	5	36	—	34	—	1	—	28	—	32	—	6	—	13	—	35	—
79	3	78	4	1	8	62	5	53	12	2	66	68	9	34	57	63	16
81	2	54	1	—	2	23	—	16	3	—	24	13	—	8	17	—	4
82	7	40	—	25	—	18	—	1	—	10	—	37	—	9	—	3	—
83	2	82	1	72	2	27	73	8	3	62	28	24	74	77	9	17	4
86	3	42	—	1	—	25	—	35	—	2	—	30	—	32	—	26	—
89	3	88	16	1	32	70	17	81	48	2	86	84	33	23	9	71	64
94	5	46	—	20	—	1	—	32	—	40	—	7	—	11	—	21	—
97	5	96	34	70	68	1	8	31	6	44	35	86	42	25	65	71	40
98	3	42	—	1	—	29	—	31	—	2	—	40	—	33	—	30	—

Modul	Basis	Indizes															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3	2	2	1														
4	3	3	1														
5	2	2	4	3	1												
6	5	5	1														
7	3	3	2	6	4	5	1										
8	3	3	1														
9	2	2	4	8	7	5	1										
10	3	3	9	7	1												
11	2	2	4	8	5	10	9	7	3	6	1						
13	2	2	4	8	3	6	12	11	9	5	10	7	1				
14	3	3	9	13	11	5	1										
16	3	3	9	11	1												
17	3	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1
18	5	5	7	17	13	11	1										
19	2	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5
22	7	7	5	13	3	21	15	17	9	19	1						
23	5	5	2	10	4	20	8	17	16	11	9	22	18	21	13	19	3
25	2	2	4	8	16	7	14	3	6	12	24	23	21	17	9	18	11
26	7	7	23	5	9	11	25	19	3	21	17	15	1				
27	2	2	4	8	16	5	10	20	13	26	25	23	19	11	22	17	7
29	2	2	4	8	16	3	6	12	24	19	9	18	7	14	28	27	25
31	3	3	9	27	19	26	16	17	20	29	25	13	8	24	10	30	28
32	3	3	9	27	17	19	25	11	1								
34	3	3	9	27	13	5	15	11	33	31	25	7	21	29	19	23	1
37	2	2	4	8	16	32	27	17	34	31	25	13	26	15	30	23	9
38	3	3	9	27	5	15	7	21	25	37	35	29	11	33	23	31	17
41	6	6	36	11	25	27	39	29	10	19	32	28	4	24	21	3	18
43	3	3	9	27	38	28	41	37	25	32	10	30	4	12	36	22	23
46	5	5	25	33	27	43	31	17	39	11	9	45	41	21	13	19	3
47	5	5	25	31	14	23	21	11	8	40	12	13	18	43	27	41	17
49	3	3	9	27	32	47	43	31	44	34	4	12	36	10	30	41	25
50	3	3	9	27	31	43	29	37	11	33	49	47	41	23	19	7	21
53	2	2	4	8	16	32	11	22	44	35	17	34	15	30	7	14	28
54	5	5	25	17	31	47	19	41	43	53	49	29	37	23	7	35	13
58	3	3	9	27	23	11	33	41	7	21	5	15	45	19	57	55	49
59	2	2	4	8	16	32	5	10	20	40	21	42	25	50	41	23	46
61	2	2	4	8	16	32	3	6	12	24	48	35	9	18	36	11	22
62	3	3	9	27	19	57	47	17	51	29	25	13	39	55	41	61	59
64	3	3	9	27	17	51	25	11	33	35	41	59	49	19	57	43	1
67	2	2	4	8	16	32	64	61	55	43	19	38	9	18	36	5	10
71	7	7	49	59	58	51	2	14	27	47	45	31	4	28	54	23	19
73	5	5	25	52	41	59	3	15	2	10	50	31	9	45	6	30	4
74	5	5	25	51	33	17	11	55	53	43	67	39	47	13	65	29	71
79	3	3	9	27	2	6	18	54	4	12	36	29	8	24	72	58	16
81	2	2	4	8	16	32	64	47	13	26	52	23	46	11	22	44	7
82	7	7	49	15	23	79	61	17	37	13	9	63	31	53	43	55	57
83	2	2	4	8	16	32	64	45	7	14	28	56	29	58	33	66	49
86	3	3	9	27	81	71	41	37	25	75	53	73	47	55	79	65	23
89	3	3	9	27	81	65	17	51	64	14	42	37	22	66	20	60	2
94	5	5	25	31	61	23	21	11	55	87	59	13	65	43	27	41	17
97	5	5	25	28	43	21	8	40	6	30	53	71	64	29	48	46	36
98	3	3	9	27	81	47	43	31	93	83	53	61	85	59	79	41	25

Modul	Basis	Zahlen																															
		17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33															
Indizes																																	
18	5	3																															
19	2	10	9																														
22	7	7	—	9	—	5																											
23	5	7	12	15	5	13	11																										
25	2	13	15	18	—	12	17	11	10																								
26	7	10	—	7	—	9	—	2	—	6																							
27	2	15	—	12	7	—	14	11	—	10	9																						
29	2	21	11	9	24	17	26	20	8	16	19	15	14																				
31	3	7	26	4	8	29	17	27	13	10	5	3	16	9	15																		
32	3	4	—	5	—	—	—	—	—	6	—	3	—	—	—																		
34	3	—	—	14	—	12	—	15	—	10	—	3	—	13	—	9	—	8															
37	2	7	17	35	25	22	31	15	29	10	12	6	34	21	14	9	5	20															
38	3	16	—	—	—	7	—	14	—	8	—	3	—	11	—	15	—	13															
41	6	33	16	9	34	14	29	36	13	4	17	5	11	7	23	28	10	18															
43	3	38	29	19	37	36	15	16	40	8	17	3	5	41	11	34	9	31															
46	5	7	—	15	—	13	—	—	—	2	—	4	—	18	—	6	—	3															
47	5	16	12	45	37	6	25	5	28	2	29	14	22	35	39	3	44	27															
49	3	25	28	35	39	—	24	38	37	16	17	3	—	18	14	7	4	41															
50	3	19	—	14	—	16	—	13	—	—	—	3	—	6	—	4	—	9															
53	2	10	35	37	49	31	7	39	20	42	25	51	16	46	13	33	5	23															
54	5	3	—	6	—	—	—	13	—	2	—	—	—	11	—	4	—	—															
58	3	21	—	13	—	9	—	4	—	20	—	3	—	—	—	17	—	6															
59	2	40	43	38	8	10	26	15	53	12	46	34	20	28	57	49	5	17															
61	2	47	13	26	24	55	16	57	9	44	41	18	51	35	29	59	5	21															
62	3	7	—	4	—	29	—	27	—	10	—	3	—	9	—	—	—	24															
64	3	4	—	13	—	—	—	—	—	6	—	3	—	—	—	—	—	8															
67	2	64	13	10	17	62	60	28	42	30	20	51	25	44	55	47	5	32															
71	7	49	58	16	40	27	37	15	44	56	45	8	13	68	60	11	30	57															
73	5	21	20	62	17	39	63	46	30	2	67	18	49	35	15	11	40	61															
74	5	5	—	25	—	26	—	21	—	2	—	30	—	15	—	27	—	4															
79	3	21	6	32	70	54	72	26	13	46	38	3	61	11	67	56	20	69															
81	2	33	—	48	25	—	14	11	—	46	9	—	18	37	—	20	5	—															
82	7	7	—	31	—	26	—	4	—	36	—	35	—	33	—	12	—	22															
83	2	56	63	47	29	80	25	60	75	54	78	52	10	12	18	38	5	14															
86	3	38	—	19	—	36	—	16	—	8	—	3	—	41	—	34	—	31															
89	3	6	18	35	14	82	12	57	49	52	39	3	25	59	87	31	80	85															
94	5	16	—	45	—	6	—	5	—	2	—	14	—	35	—	3	—	27															
97	5	89	78	81	69	5	24	77	76	2	59	18	3	13	9	46	74	60															
98	3	25	—	35	—	—	—	38	—	16	—	3	—	18	—	7	—	41															

[illegible]

Modul	Basis	Zahlen																			
		34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50			
		Indizes																			
37	2	8	19	18																	
38	3	—	10	—	9																
41	6	19	21	2	32	35	6	20													
43	3	23	18	14	7	4	33	22													
46	5	—	20	—	21	—	8	—	12	—	5	—	11								
47	5	34	33	30	42	17	31	9	15	24	13	43	41	23							
49	3	9	—	12	32	19	34	23	15	—	6	8	31	22	5	21					
50	3	—	—	—	7	—	18	—	12	—	5	—	—	—	11	—	10				
53	2	11	9	36	30	38	41	50	45	32	22	8	29	40	44	21	28	43			
54	5	—	15	—	12	—	—	—	7	—	8	—	—	—	5	—	10	—			
58	3	—	18	—	23	—	27	—	7	—	25	—	12	—	19	—	16	—			
59	2	41	24	44	55	39	37	9	14	11	33	27	48	16	23	54	36	13			
61	2	48	11	14	39	27	46	25	54	56	43	17	34	58	20	10	38	45			
62	3	—	18	—	25	—	12	—	14	—	19	—	22	—	6	—	26	—			
64	3	—	9	—	—	—	—	—	10	—	15	—	—	—	—	—	12	—			
67	2	65	38	14	22	11	58	18	53	63	9	61	27	29	50	43	46	31			
71	7	55	29	64	20	22	65	46	25	33	48	43	10	21	9	50	2	62			
73	5	29	34	28	64	70	65	25	4	47	51	71	13	54	31	38	66	10			
74	5	—	29	—	—	—	11	—	22	—	9	—	33	—	12	—	20	—			
79	3	25	37	10	19	36	35	74	75	58	49	76	64	30	59	17	28	50			
81	2	34	39	—	42	49	—	26	53	—	22	15	—	12	7	—	32	47			
82	7	—	19	—	8	—	34	—	—	—	14	—	28	—	39	—	2	—			
83	2	57	35	64	20	48	67	30	40	81	71	26	7	61	23	76	16	55			
86	3	—	18	—	7	—	33	—	6	—	—	—	27	—	12	—	28	—			
89	3	22	63	34	11	51	24	30	21	10	29	28	72	73	54	65	74	68			
94	5	—	33	—	42	—	31	—	15	—	13	—	41	—	—	—	18	—			
97	5	27	32	16	91	19	95	7	85	39	4	58	45	15	84	14	62	36			
98	3	—	—	—	32	—	34	—	15	—	6	—	31	—	5	—	—	—			

Modul	Basis	Indizes														
		34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
		Zahlen														
37	2	28	19	1												
38	3															
41	6	20	38	23	15	8	7	1								
43	3	31	7	21	20	17	8	24	29	1						
46	5								.							
47	5	34	29	4	20	6	30	9	45	37	44	32	19	1		
49	3	39	19	8	24	23	20	11	33	1						
50	3															
53	2	9	18	36	19	38	23	46	39	25	50	47	41	29	5	10
54	5															
58	3															
59	2	27	54	49	39	19	38	17	34	9	18	36	13	26	52	45
61	2	45	29	58	55	49	37	13	26	52	43	25	50	39	17	34
62	3															
64	3															
67	2	65	63	59	51	35	3	6	12	24	48	29	58	49	31	62
71	7	10	70	64	22	12	13	20	69	57	44	24	26	40	67	43
73	5	35	29	72	68	48	21	32	14	70	58	71	63	23	42	64
74	5	3	15	1												
79	3	13	39	38	35	26	78	76	70	52	77	73	61	25	75	67
81	2	34	68	55	29	58	35	70	59	37	74	67	53	25	50	19
82	7	39	27	25	11	77	47	1								
83	2	59	35	70	57	31	62	41	82	81	79	75	67	51	19	38
86	3	31	7	21	63	17	51	67	29	1						
89	3	36	19	57	82	68	26	78	56	79	59	88	86	80	62	8
94	5	81	29	51	67	53	77	9	45	37	91	79	19	1		
97	5	2	10	50	56	86	42	16	80	12	60	9	45	31	58	96
98	3	39	19	57	73	23	69	11	33	1						

Modul	Basis	Zahlen																
		51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67
		Indizes																
53	2	27	26															
54	5	—	—	9														
58	3	22	—	24	—	15	—	14										
59	2	32	47	22	35	31	21	30	29									
61	2	53	42	33	19	37	52	32	36	31	30							
62	3	8	—	17	—	13	—	5	—	16	—	15						
64	3	5	—	—	—	—	—	14	—	11	—	—	—	—				
67	2	37	21	57	52	8	26	49	45	36	56	7	48	35	6	34	33	
71	7	5	51	23	14	59	19	42	4	3	66	69	17	53	36	67	63	47
73	5	27	3	53	26	56	57	68	43	5	23	58	19	45	48	60	69	50
74	5	3	—	8	—	7	—	23	—	17	—	31	—	24	—	14	—	10
79	3	22	42	77	7	52	65	33	15	31	71	45	60	55	24	18	73	48
81	2	—	10	45	—	36	19	—	38	41	—	52	21	—	6	31	—	44
82	7	32	—	13	—	15	—	16	—	24	—	6	—	11	—	27	—	23
83	2	46	79	59	53	51	11	37	13	34	19	66	39	70	6	22	15	45
86	3	39	—	10	—	13	—	20	—	24	—	29	—	37	—	15	—	40
89	3	7	55	78	19	66	41	36	75	43	15	69	47	83	8	5	13	56
94	5	36	—	38	—	8	—	19	—	10	—	4	—	26	—	12	—	37
97	5	63	93	10	52	87	37	55	47	67	43	64	80	75	12	26	94	57
98	3	26	—	10	—	27	—	36	—	13	—	11	—	—	—	20	—	28
		Indizes																
		Zahlen																
		68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84
		Indizes																
71	7	61	41	35														
73	5	37	52	42	44	36												
74	5	—	19	—	16	—	18											
79	3	29	27	41	51	14	44	23	47	40	43	39						
81	2	35	—	40	51	—	30	43	—	50	29	—	28	27				
82	7	—	29	—	17	—	30	—	21	—	38	—	5	—	20			
83	2	58	50	36	33	65	69	21	44	49	32	68	43	31	42	41		
86	3	—	17	—	5	—	11	—	9	—	23	—	14	—	4	—	22	—
89	3	38	58	79	62	50	20	27	53	67	77	40	42	46	4	37	61	26
94	5	—	25	—	28	—	29	—	22	—	39	—	44	—	34	—	30	—
97	5	61	51	66	11	50	28	29	72	53	21	33	30	41	88	23	17	73
98	3	—	39	—	24	—	37	—	17	—	—	—	14	—	4	—	9	—
		Indizes																
		Zahlen																
		85	86	87	88	89	90	91	92	93	94	95	96	97				
		Indizes																
86	3	21																
89	3	76	45	60	44													
94	5	17	—	9	—	24	—	43	—	23								
97	5	90	38	83	92	54	79	56	49	20	22	82	48					
98	3	12	—	19	—	23	—	—	—	8	—	22	—	21				

Modul	Basis	Indizes																
		51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67
		Zahlen																
53	2	27	1															
54	5																	
58	3																	
59	2	6	12	24	48	37	15	30	1									
61	2	28	56	51	41	21	42	23	46	31	1							
62	3																	
64	3																	
67	2	27	54	41	15	30	60	53	39	11	22	44	21	42	17	34	1	
71	7	52	9	63	15	34	25	33	18	55	30	68	50	66	36	39	60	65
73	5	43	69	53	46	11	55	56	61	13	65	33	19	22	37	39	49	26
74	5																	
79	3	71	55	7	21	63	31	14	42	47	62	28	5	15	45	56	10	30
81	2	71	61	41	1													
82	7																	
83	2	55	27	54	25	50	17	34	68	53	23	46	9	18	36	72	61	39
86	3																	
89	3	38	25	75	47	52	67	23	69	29	87	83	71	35	16	48	55	76
94	5																	
97	5	69	54	76	89	57	91	67	44	26	33	68	49	51	61	14	70	59
98	3																	
Modul	Basis	Indizes																
		68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84
		Zahlen																
71	7	29	61	1														
73	5	57	66	38	44	1												
74	5																	
79	3	11	33	20	60	22	66	40	41	44	53	1						
81	2																	
82	7																	
83	2	78	73	63	43	3	6	12	24	48	13	26	52	21	42	1		
86	3																	
89	3	50	61	5	15	45	46	49	58	85	77	53	70	32	7	21	63	11
94	5																	
97	5	4	20	3	15	75	84	32	63	24	23	18	90	62	19	95	87	47
98	3																	
Modul	Basis	Indizes																
		85	86	87	88	89	90	91	92	93	94	95	96	97				
		Zahlen																
86	3																	
89	3	33	10	30	1													
94	5																	
97	5	41	11	55	81	17	85	37	88	52	66	39	1					
98	3																	

IV. Die kleinste Lösung der Gleichung $x^2 - ay^2 = \pm 1$
für die unter 100 liegenden Werte von a .

[Wenn die Zahl a mit dem Zeichen * versehen ist, so gelten die entsprechenden Werte $x = \xi$, $y = \eta$ für die Gleichung $x^2 - ay^2 = -1$.
Es ist dann $x = 2\xi^2 + 1$, $y = 2\xi\eta$ die kleinste Lösung der Gleichung $x^2 - ay^2 = +1$.] (§. 68.)

a	x	y	a	x	y	a	x	y
2*	1	1	38	37	6	71	3480	413
3	2	1	39	25	4	72	17	2
5*	2	1	40	19	3	73*	1068	125
6	5	2	41*	32	5	74*	43	5
7	8	3	42	13	2	75	26	3
8	3	1	43	3482	531	76	57799	6630
10*	3	1	44	199	30	77	351	40
11	10	3	45	161	24	78	53	6
12	7	2	46	24335	3588	79	80	9
13*	18	5	47	48	7	80	9	1
14	15	4	48	7	1	82*	9	1
15	4	1	50*	7	1	83	82	9
17*	4	1	51	50	7	84	55	6
18	17	4	52	649	90	85*	378	41
19	170	39	53*	182	25	86	10405	1122
20	9	2	54	485	66	87	28	3
21	55	12	55	89	12	88	197	21
22	197	42	56	15	2	89*	500	53
23	24	5	57	151	20	90	19	2
24	5	1	58*	99	13	91	1574	165
26*	5	1	59	530	69	92	1151	120
27	26	5	60	31	4	93	12151	1260
28	127	24	61*	29718	3805	94	2543295	221064
29*	70	13	62	63	8	95	39	4
30	11	2	63	8	1	96	49	5
31	1520	273	65*	8	1	97*	5604	569
32	17	3	66	65	8	98	99	10
33	23	4	67	48842	5967	99	10	1
34	35	6	68	33	4			
35	6	1	69	7775	936			
37*	6	1	70	251	30			

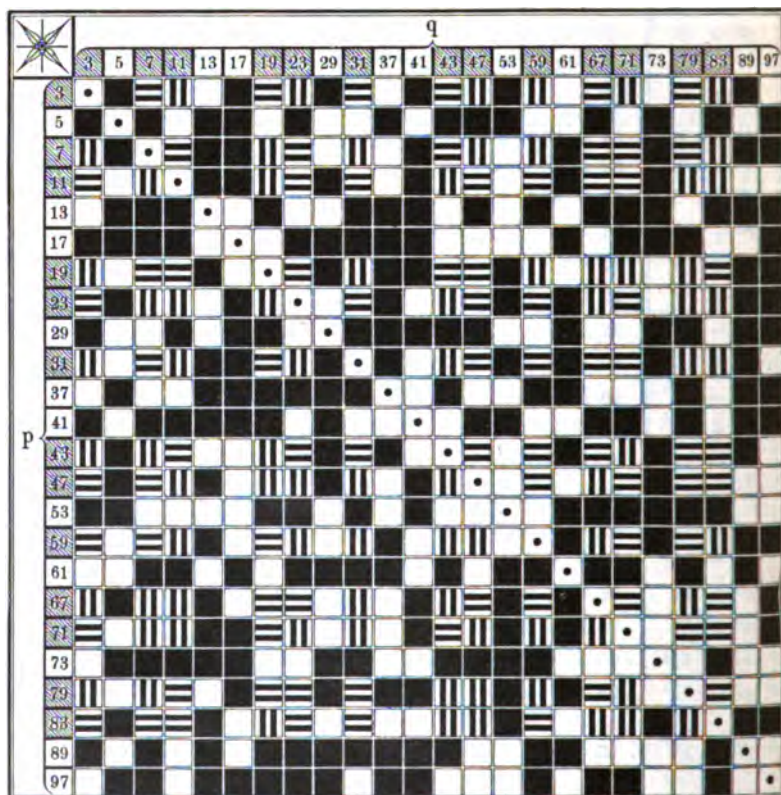
V. Die Formen der Divisoren von $x^3 \pm a$
für die Werte von $a = 1$ bis $a = 23$. (§. 121 und 122.)

$x^3 + 1$	$4k + 1.$
$x^3 + 2$	$8k + 1, 3.$
$x^3 - 2$	$8k + 1, 7.$
$x^3 + 3$	$12k + 1, 7.$
$x^3 - 3$	$12k + 1, 11.$
$x^3 + 5$	$20k + 1, 3, 7, 9.$
$x^3 - 5$	$20k + 1, 9, 11, 19.$
$x^3 + 6$	$24k + 1, 5, 7, 11.$
$x^3 - 6$	$24k + 1, 5, 19, 23.$
$x^3 + 7$	$28k + 1, 9, 11, 15, 23, 25.$
$x^3 - 7$	$28k + 1, 3, 9, 19, 25, 27.$
$x^3 + 10$	$40k + 1, 7, 9, 11, 13, 19, 23, 37.$
$x^3 - 10$	$40k + 1, 3, 9, 13, 27, 31, 37, 39.$
$x^3 + 11$	$44k + 1, 3, 5, 9, 15, 23, 25, 27, 31, 37.$
$x^3 - 11$	$44k + 1, 5, 7, 9, 19, 25, 35, 37, 39, 43.$
$x^3 + 13$	$52k + 1, 7, 9, 11, 15, 17, 19, 25, 29, 31, 47, 49.$
$x^3 - 13$	$52k + 1, 3, 9, 17, 23, 25, 27, 29, 35, 43, 49, 51.$
$x^3 + 14$	$56k + 1, 3, 5, 9, 13, 15, 19, 23, 25, 27, 39, 45.$
$x^3 - 14$	$56k + 1, 5, 9, 11, 13, 25, 31, 43, 45, 47, 51, 55.$
$x^3 + 15$	$60k + 1, 17, 19, 23, 31, 47, 49, 53.$
$x^3 - 15$	$60k + 1, 7, 11, 17, 43, 49, 53, 59.$
$x^3 + 17$	$68k + 1, 3, 7, 9, 11, 13, 21, 23, 25, 27, 31, 33, 39, 49, 53, 63.$
$x^3 - 17$	$68k + 1, 9, 13, 15, 19, 21, 25, 33, 35, 43, 47, 49, 53, 55, 59, 67.$
$x^3 + 19$	$76k + 1, 5, 7, 9, 11, 17, 23, 25, 35, 39, 43, 45, 47, 49, 55, 61, 63, 73.$
$x^3 - 19$	$76k + 1, 3, 5, 9, 15, 17, 25, 27, 31, 45, 49, 51, 59, 61, 67, 71, 73, 75.$
$x^3 + 21$	$84k + 1, 5, 11, 17, 19, 23, 25, 31, 37, 41, 55, 71.$
$x^3 - 21$	$84k + 1, 5, 17, 25, 37, 41, 43, 47, 59, 67, 79, 83.$
$x^3 + 22$	$88k + 1, 9, 13, 15, 19, 21, 23, 25, 29, 31, 35, 43, 47, 49, 51, 61, 71, 81, 83, 85.$
$x^3 - 22$	$88k + 1, 3, 7, 9, 13, 21, 25, 27, 29, 39, 49, 59, 61, 63, 67, 75, 79, 81, 85, 87.$
$x^3 + 23$	$92k + 1, 3, 9, 13, 25, 27, 29, 31, 35, 39, 41, 47, 49, 55, 59, 71, 73, 75, 77, 81, 85, 87.$
$x^3 - 23$	$92k + 1, 7, 9, 11, 13, 15, 19, 25, 29, 41, 43, 49, 51, 63, 67, 73, 77, 79, 81, 83, 85, 91.$

422 Graphische Darstellung des Reziprozitätssatzes etc.

VI. Graphische Darstellung des Reziprozitätssatzes
für alle Primzahlen unter 100.

(Nach A. Matrot.)



Zeichenerklärung:

Die Felder mit den Primzahlen p, q der Form $4n + 3$ sind schraffiert, die mit den Primzahlen der Form $4n + 1$ nicht.

	q ist	
	Rest von p	Nichtrest von p
Wenigstens eine der Primzahlen p, q hat die Form $4n + 1$.		
Beide Primzahlen p, q haben die Form $4n + 3$.		

NAMEN- UND SACHREGISTER.

A.

- Alkarchi, Abū Bekr Muhammed ibn Alhusain (gest. gegen 1029 n. Chr.) 72, 324.
 Anzahl der Primzahlen 8.
 — — — unterhalb einer gegebenen Zahl 58.
 — der Zahlen eines Gebiets, welche durch gegebene Primzahlen nicht teilbar sind 54.

B.

- Bachet, Claude Gaspar B. de Méziriac (1687—1638) 90, 93, 393.
 Bachetscher Satz 393.
 Bachmann, Paul Gustav Heinrich (geb. 1837) 27.
 Bakhshālī, das Rechenbuch von 148.
 Baumgart, Oswald 361.
 Befreundete Zahlen 32.
 Beha-eddin siehe unter Muhammed.
 Bernoulli, Johann (1667—1748) 302.
 Bhāskara, Acārya (geb. 1114 n. Chr.) 85, 108, 135, 158, 220, 221.
 Biernatzki, K. L. 103.
 Binet, Jacques Philippe Marie (1786—1856) 125.
 Blater, Joseph (geb. 1839) 271.
 Bombelli, Rafaele (seine „Algebra“ erschien 1572) 164.
 Bork, Heinrich 309.
 Bouvelles, Charles de (1470—1553) 30.
 Brahme Gupta (geb. 598 n. Chr.) 220.
 Braun, Johann Mathias Julius (geb. 1864) 59.

- Brouncker, Lord William (1620—1684) 165, 219.
 Brüche, rationale, Verwandlung in Dezimalbrüche 303.
 — — — in Kettenbrüche 169.
 Bungus, Petrus (etwa 1550—1601) 7.
 Burckhardt, Jean Charles (1773—1825) 13.

C.

- Canon arithmeticus von K. G. J. Jacobi 245.
 Cantor, Moritz (geb. 1829) 32, 140, 197.
 Cardano, Hieronimo (1501—1576) 147.
 Cataldi, Pietro Antonio (etwa 1543—1626) 30, 164.
 Cauchy, Augustin Louis (1789—1857) 361.
 Chinesen 103.
 Chuquet, Nicolas (Le Triparty en la science des nombres verfaßt 1484) 324.
 Colebrooke, Henry Thomas (1756—1837) 85.
 Congruens und Congruum bei Leonardo Pisano, Paciulo und Ghaligai 64.
 Congruente Zahlen und Congruenzen siehe unter Kongruente Zahlen und Kongruenzen.
 Cyklische Methode der Inder 220.

D.

- Darstellung der Zahlen als Differenz zweier Quadrate 17.

Darstellung der Zahlen als Summe
aufeinander folgender Zahlen 16, 400.
— — — als Summe von Quadraten
189, 849, 393.
Dase, Johann Martin Zacharias (1824—
1861) 13.
Dezimalbrüche, Verwandlung ge-
meiner Brüche in 308.
Diophant von Alexandria (um 275
n. Chr.) 93, 140, 141, 142, 143, 144,
146, 148, 393, 401.
Dirichlet, Peter Gustav Lejeune
(1805—1859) 10, 123, 140, 225.
Divisoren einer Zahl 7, 23.
— — Form 346.
— von $a^m \pm 1$ 297.
— — $x^2 - a$ 367.
Divisor, größter gemeinschaftlicher,
von Zahlen 32.
Dyadisches Zahlensystem 3.

E.

Eigentliche Divisoren einer Zahl 7.
Eisenstein, Ferdinand Gotthold Max
(1823—1852) 361.
Eneström, Gustaf (geb. 1852) 402.
Epstein, Paul (geb. 1871) 258, 402.
Eratosthenes (um 240 v. Chr.) 11.
Euklid (um 300 v. Chr.) 7, 8, 20, 27,
28, 33, 34, 39.
Euler, Leonhard (1707—1783) 9, 14,
27, 32, 42, 93, 113, 120, 124, 140,
141, 145, 146, 149, 150, 161, 195,
196, 219, 232, 238, 243, 257, 269, 302,
322, 332, 334, 347, 361, 393, 394, 402.
Exponent, zu dem eine Zahl für
einen Modul gehört 228, 268.
Exponent und Indizes einer Zahl
253.
— Produkt der zu demselben Expo-
nenten gehörenden Zahlen 238.
— Summe dieser Zahlen 259.
Exponentialkongruenz 250.

F.

Faktoren, Zerlegung in 19, 297, 367.
Fermat, Pierre de (1601—1665) 11, 14,
19, 26, 31, 124, 140, 150, 219, 220,
265, 300, 302, 351, 393.

Fermatsche Aufgabe 219.
Fermatscher Satz 119, 232.
— —, Verallgemeinerung desselben
269, 335.
Formen der Primzahlen 7.
— der Zahlen 6.
Frenicle, Bernard Fr. de Bessy (etwa
1602—1675) 32, 124, 138.
Funktion φ , die 42, 401.

G.

Gauß, Karl Friedrich (1777—1855)
20, 47, 59, 79, 95, 99, 116, 123, 303,
335, 343, 355, 361, 362, 367, 378, 393.
Ghaligai, Francesco (Die Summa de
arithmetica erschien 1521) 64.
Girard, Albert (gest. 1632) 38.
Glaisher, James Whitbread Lee
(geb. 1848) 13.
Gleichungen, unbestimmte, ersten
Grades 90.
— — zweiten Grades 134 ff.
Goldbach, Christian (1690—1764) 10.
Gram, Jörgen Pedersen (geb. 1850) 13.
Grohmann, Eduard 77.

H.

Hankel, Hermann (1839—1873) 220.
Heis, Eduard (1806—1877) 154, 155.
Heron von Alexandria (um 110
v. Chr.) 140.
Heronische Zahlen 140, 222.
Hill, George William (geb. 1838) 75.
Hirsch, Meier (1765—1851) 153, 157.
Hoche, Richard 103.
Hochheim, Karl Adolf (geb. 1840)
72, 324.

I.

Ibn Esra, Abraham (1092—1167) 324.
Inder 71, 93.
Indizes für Primzahlen 243.
— für Potenzen ungerader Prim-
zahlen und das doppelte solcher
Potenzen 287.
— für Potenzen von 2 292.
— einer Zahl für verschiedene Basen
251.

Indizes, Summe der kleinsten Indizes einer Zahl 258, 402.
— und Exponent 258.
Irrationale Größen, Verwandlung in Kettenbrüche 198, 202, 208.

J.

Jacobi, Karl Gustav Jacob (1804—1851) 245, 361.

K.

Kelsler, Friedrich Christian Ludwig (1824—1896) 309.
Kettenbrüche, Definition der 165.
— Erfindung der 164.
— periodische 200.
— symmetrische 187.
— Umkehrung der 185.
— Verwandlung irrationaler Größen in 198, 202, 208.
— — von Quadratwurzeln in 213.
Konen, Heinrich (geb. 1874) 220.
Kongruente Zahlen 64.
Kongruenzen 67.
—, Auflösung durch Probieren 83.
—, Umformung der 81.
—, Verbindung der 67.
—, Wurzeln der 82.
Kongruenz ersten Grades, Anwendungen der 96.
— — —, Auflösung der 88, 125, 196, 245, 271, 287, 294.
— — —, Möglichkeit der 85.
— — — mit mehreren Unbekannten 108.
— — — mit zusammengesetzten Moduli 94.
Kongruenzen ersten Grades, ein System von 111.
—, binomische 247, 287, 294, 295.
—, quadratische, Verwandlung gemischt quadratischer in rein quadratische 318.
—, —, Auflösung der rein quadratischen 317, 341, 378.
—, —, Auflösung der Kongruenz $ax^2 + by^2 \equiv c \pmod{p}$ 388.
Kriterium zur Unterscheidung der

quadratischen Reste und Nichtreste, das Euler'sche 332, das Gauß'sche 355.
Kronecker, Leopold (1823—1891) 361.
Kummer, Ernst Eduard (1810—1893) 140.

L.

Lagrange, Jos. Louis (1736—1812) 14, 114, 118, 121, 124, 137, 141, 165, 196, 220, 351, 393.
Lambert, Johann Heinrich (1728—1777) 120.
Landau, Edmund Georg Hermann (geb. 1877) 401.
Laplace, Pierre Simon (1749—1827) 122, 125.
Legendre, Adrien Marie (1752—1833) 5, 11, 14, 31, 32, 50, 54, 59, 225, 238, 333, 361, 367, 393, 399.
Legendresche Symbol, Das 335.
Leibniz, Gottfried Wilhelm (1661—1716) 5, 7, 38, 123.
Le Lasseur 32.
Leonardo Pisano (Fibonacci) (der Liber Abaci verfaßt 1202, der Liber quadratorum 1225) 11, 38, 64, 65, 72, 103, 147.
Liouville, Joseph (1809—1882) 361.
Lucas, Edouard (1842—1891) 29, 32.

M.

Mangelhafte Zahlen ($\acute{\alpha}\rho\iota\theta\mu\omicron\iota \acute{\epsilon}\lambda\lambda\omicron\pi\epsilon\iota\varsigma$) 27.
Marre, Eugène Aristide (geb. 1823) 324.
Matrot, Adolphe (gest. 1897) 391, 396, 422.
Meißel, Daniel Friedrich Ernst (1826—1895) 59.
Mertens, Franz Carl Joseph (geb. 1840) 59.
Modul, der 64.
Muhammed Beha-eddin Alhossain (1547—1622) 402.
— ibn Musa Alchwarizmi (gestorben zwischen 835 und 845) 72.

Mylon, Claude, ein in Paris wohnender Jurist, der 1656—1660 mit Huygens in Briefwechsel stand 32.

N.

Näherungsbrüche von Kettenbrüchen, Bildung der 173.

— — —, Eigenschaften der 178.

— — —, eingeschaltete 182.

Nesselmann, G. H. F. 402.

Nessnerprobe, die 72.

Nichtreste, quadratische 322.

Nikomachus von Gerasa (um 100 v. Chr.) 7, 11, 27, 30, 103, 160.

O.

Osterfest, Berechnung des Ostersonntags 79.

Ostrogradsky, Michael Vasiljewitch (1801—1861) 245.

P.

Paciuolo, Lucas (etwa 1445 bis etwa 1509) 64, 147.

Partialbrüche, Zerlegung in 103, 110.

Pell, John (1610—1685) 220, 402.

Periode einer Zahl 230, 236, 269.

Periodizität der Reihe der Potenzreste 230, 269.

Planudes, Maximus (um 1330) 72 137.

Polynome, Darstellung der Primzahlen durch 13.

Potenz, höchste, einer Primzahl, die in $n!$ aufgeht 50.

Potenzen von 2 als Moduln 262.

— ungerader Primzahlen als Moduln 287.

Potenzreste, Berechnung der 227.

— für Primzahlmoduln 227.

— für zusammengesetzte Moduln 263.

Primitive Wurzeln von Primzahlen 238.

— —, Berechnung derselben 240.

— —, Produkt derselben 258.

— —, Summe derselben 262.

Primitive Wurzeln der Potenzen von Primzahlen 277.

— — des Doppelten solcher Potenzen 283.

— — der Potenzen von 2 292.

— —, Zahlen ohne 275.

Primzahlen, Anzahl der 8.

—, Darstellung durch Polynome 13.

—, Definition 7.

— gleicher Differenz 14.

—, Ermittlung der 11, 270.

—, relative 33, 35.

Primzahlenmenge in einem gegebenen Gebiet 58.

Probieren, Auflösung der Kongruenzen durch 83.

Produkt der zu demselben Exponenten gehörenden Zahlen 238.

— der primitiven Wurzeln einer Primzahl 258.

— der Zahlen, die prim zu p^1 und $< p^2$ sind 331.

—, Quadratischer Charakter eines 335.

Pythagoreische Gleichung 137.

Q.

Quadrate, Zerfällung der Zahlen in zwei 189, 349.

—, Zerfällung in 4 oder weniger 393.

Quadratische Kongruenz, Auflösung 317, 341, 378.

Quadratwurzeln, Verwandlung in Kettenbrüche 213.

Quotienten eines Kettenbruchs 173.

R.

Rechnungsproben 71.

Reste einer Zahl für einen Modul 65.

—, quadratische 322.

—, Aufeinanderfolge derselben bei Primzahlen 335.

—, Moduln, für welche -1 quadratischer Rest ist 347, 357, 391.

—, Moduln, für welche $+2$ quadratischer Rest ist 350, 357, 391.

—, Moduln, für welche 3 quadratischer Rest ist 358.

— — ungerader Primzahlen 325.

Reste, quadratische, der Potenzen ungerader Primzahlen 327.

— der Potenzen von 2 338.

Restproblem, das 98.

Restsystem, das vollständige 66.

Reziprozitätssatz, der 360.

Riemann, Georg Friedrich Bernhard (1826—1866) 59.

S.

Scheibner, Wilhelm (geb. 1826) 59.

Schering, Ernst Christian Julius (1833—1897) 361.

Schwenker, Daniel (1585—1636) 164.

Seelhoff, Paul Peter Heinrich (1829—1896) 90, 303.

Sieb des Eratosthenes 11.

Silberberg, Moritz (geb. 1867) 324.

Stern, Moritz Abraham (1807—1894) 117.

Straufs, Emil (1859—1892) 48.

Sylvester, James Joseph (1814—1897) 400.

T.

Tābit ibn Kurrah (826—901) 32.

Teilbarkeitsregeln 72.

Teilerfremde Zahlen 33.

Thacker, A. 45.

Tschebyscheff, Pafnutij (1821—1894) 59, 243.

U.

Überschiefsende Zahlen (*ἀρῖθμοὶ ἐπερτίζεις*) 27.

Unbestimmte Gleichungen ersten Grades 90.

— — zweiten Grades 134 ff.

Uneigentliche Divisoren einer Zahl 7.

V.

Vacca, Giovanni (geb. 1872) 7, 123.

Verteilung der Zahlen unter die Divisoren von $q(m)$ als Exponenten 233, 271, 289.

Vielfache, das kleinste — von Zahlen 38.

—, Summe der Reste aller — einer Zahl 126.

Vollkommene Zahlen (*ἀρῖθμοὶ τέλειοι*) 27.

W.

Wallis, John (1616—1703) 26, 165, 219.

Waring, Edward (1736—1798) 14, 118.

Wertheim, Gustav (geb. 1843) 26, 45, 75, 93, 97, 243, 402.

Wilson, John 118.

Wilsonsche Satz, der 114, 124, 129, 257.

— —, Verallgemeinerung desselben 332, 343, 402, 406.

Wurzeln von Kongruenzen 82.

—, Anzahl der Wurzeln einer Kongruenz, deren Modul eine Primzahl ist 127.

Z.

Zahlensysteme 1.

Zauberkarten 5.

Zeller, Christian Julius Johannes (1824—1899) 361.

Zerstäubungsmethode der Inder 197.

Ziffern 1.

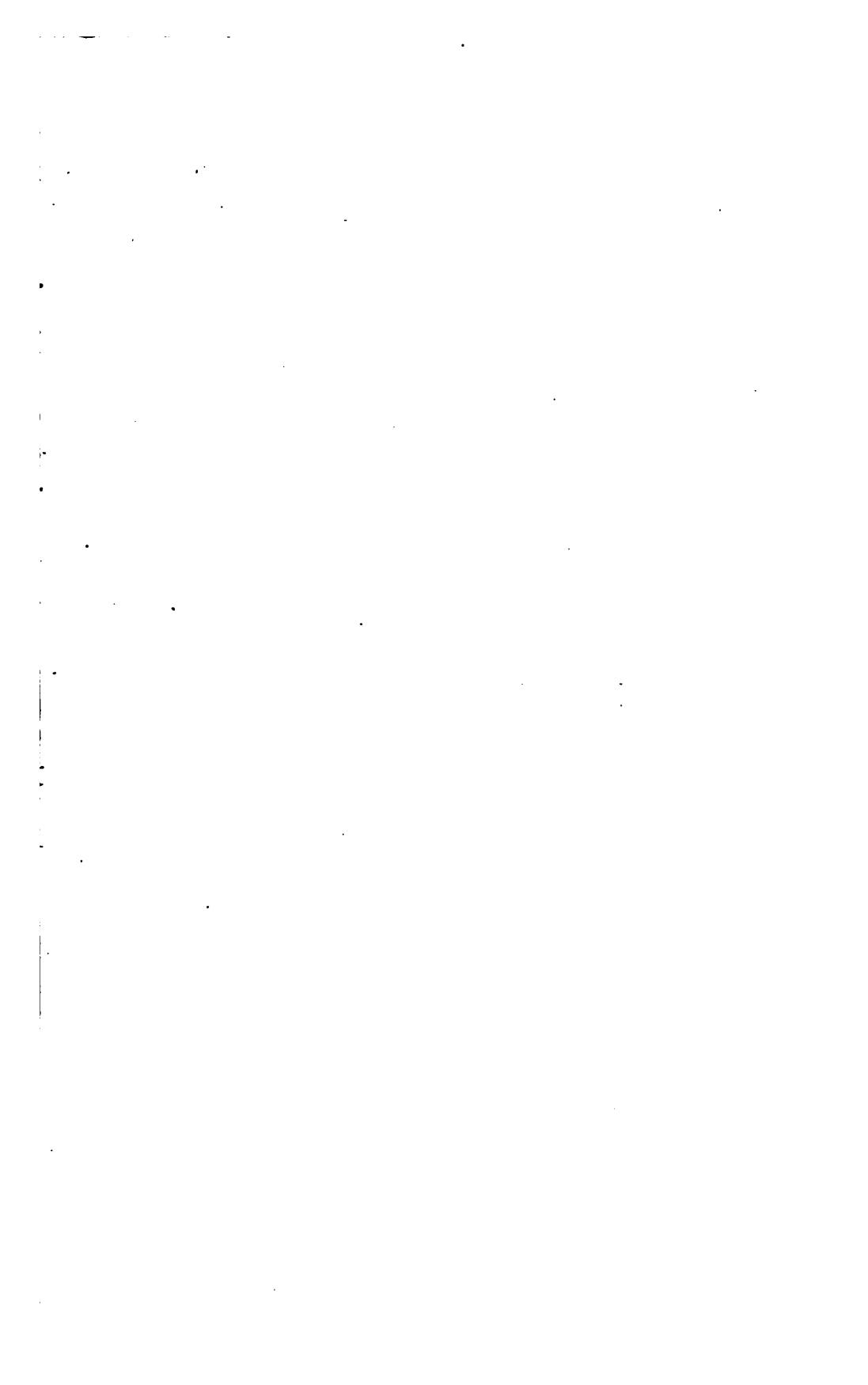
Zusammengesetzte Zahlen, Definition 7.

— —, Zerlegung in Faktoren 19, 297, 308, 367.

Berichtigungen.

Seite 85, Zeile 10 von unten lies: „der der Sache nach schon u. s. w.“,
statt „der Sache nach der schon u. s. w.“

Seite 318, Zeile 1 von oben lies: $1 + E\left(\frac{m}{4}\right)$.





~~DUE JUN 20 1933~~

~~DUE JUN 15 1933~~

~~DUE OCT 25 31~~

DUE JAN 21 1938

~~DUE JUN 25 1932~~

~~DUE JUN 25 1932~~